Guide d'administration de vShield

vShield Manager 5.0.1
vShield App 5.0.1
vShield Edge 5.0.1
vShield Endpoint 5.0.1

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-000838-00

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

http://www.vmware.com/fr/support/pubs/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

Copyright © 2010 – 2012 VMware, Inc. Tous droits réservés. Ce produit est protégé par les lois américaines et internationales relatives au copyright et à la propriété intellectuelle. Les produits VMware sont protégés par un ou plusieurs brevets répertoriés à l'adresse http://www.vmware.com/go/patents-fr.

VMware est une marque déposée ou une marque de VMware, Inc. aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et noms mentionnés sont des marques déposées par leurs propriétaires respectifs.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

Guide d'administration vShield 7

1 Vue générale de vShield 9
- À propos des composants vShield 9
- Migration des composants vShield 11
- À propos de VMware Tools sur les composants vShield 11
- Ports nécessaires pour la communication vShield 11

2 Bases de l'interface utilisateur de vShield Manager 13
- Se connecter à l'interface utilisateur de vShield Manager 13
- À propos de l'interface utilisateur de vShield Manager 14

3 Paramètres du système de gestion 17
- Connexion à vCenter Server 17
- Enregistrer vShield Manager comme plug-in vSphere Client 18
- Identifier les services DNS 18
- Régler la date et l'heure de vShield Manager 19
- Télécharger les journaux du support technique de vShield 19
- Afficher l'état de vShield Manager 19
- Ajouter un certificat SSL pour identifier le service Web vShield Manager 20

4 Gestion d'utilisateurs 21
- Gestion des comptes d'utilisateur 21
- Gestion du compte d'utilisateur par défaut 22
- Ajouter un compte d'utilisateur 22
- Modifier un compte d'utilisateur 23
- Changer un rôle d'utilisateur 24
- Désactiver ou activer un compte d'utilisateur 24
- Supprimer un compte d'utilisateur 24

5 Mise à jour du logiciel système 25
- Afficher le logiciel système en cours 25
- Envoyer une mise à jour 25

6 Sauvegarde des données de vShield Manager 27
- Sauvegarde sur demande de vos données vShield Manager 27
- Programmer une sauvegarde des données de vShield Manager 28
- Restaurer une sauvegarde 29

7 Événements système et journaux d'audit 31
- Afficher le rapport d'événements système 31

Événements de dispositif virtuel vShield Manager 31
Événements vShield App 32
À propos du format Syslog 33
Afficher le journal d'audit 33

8 Gestion de vShield Edge 35
Afficher l'état d'un vShield Edge 35
Spécifier un serveur Syslog distant 36
Gestion du pare-feu vShield Edge 36
Gestion des règles NAT 40
Gestion du service DHCP 41
Gestion du service VPN 43
Ajouter une route statique. 45
Gérer le service d'équilibrage de charge 46
Démarrer ou arrêter les services vShield Edge 47
Redéployer vShield Edge 47

9 Gestion de vShield App 49
Envoi des événements système vShield App à un serveur Syslog 49
Affichage de l'état système en cours d'une vShield App 50
Redémarrer une vShield App 50
Forcer la synchronisation d'une vShield App avec vShield Manager 50
Affichage des statistiques du trafic en fonction de l'interface vShield App 51
Configuration du mode Prévention de défaillance du pare-feu vShield App 51
Exclusion de machines virtuelles de la protection vShield App 51
Télécharger les journaux du support technique de vShield App 52

10 vShield App Flow Monitoring 53
Description de l'affichage Flow Monitoring 53
Changement de la plage de dates dans les graphiques de Flow Monitoring 54
Afficher une application spécifique dans les graphiques Flow Monitoring 54
Afficher le rapport de Flow Monitoring 55
Supprimer tous les flux enregistrés 56

11 Gestion du pare-feu vShield App 59
Utilisation de App Firewall 59
Utilisation des applications 61
Regroupement des objets 63
Utilisation desrègles de pare-feu d'application 64
Utilisation de SpoofGuard 65

12 Événement et alarmes vShield Endpoint 69
Afficher l'état de vShield Endpoint 69
Alarmes vShield Endpoint 70
Événements de vShield Endpoint 70
Messages d'audit de vShield Endpoint 71

13 Gestion de vShield Data Security 73
Rôles d'utilisateur vShield Data Security 74
Définition d'une stratégie de sécurité des données 74
Modification d'une stratégie de sécurité des données 76
Exécution d'une analyse de la sécurité des données 77
Affichage et téléchargement des rapports 77
Création d'expressions ordinaires 78
Réglementations disponibles 79
Lames d'analyse de contenu disponibles 96
Formats de fichier pris en charge 117

14 Dépannage 123
Résoudre les problèmes d'installation de vShield Manager 123
Résoudre les problèmes de fonctionnement 124
Résoudre les problèmes liés à vShield Edge 126
Résoudre les problèmes liés à vShield Endpoint 127
Résolution des problèmes liés à vShield Data Security 128

Index 131

Guide d'administration vShield

Le *Guide d'administration vShield* explique comment installer, configurer, surveiller et gérer d'une part le système VMware® vShield™ en utilisant l'interface utilisateur vShield Manager, le plug-in vSphere Client, d'autre part l'interface de ligne de commande (CLI). Il inclut des instructions de configuration pas à pas et des suggestions de meilleures pratiques.

Public cible

Ce manuel est destiné à toute personne souhaitant installer ou utiliser vShield dans un environnement VMware vCenter. Les informations qu'il contient sont destinées aux administrateurs système familiarisés avec la technologie des machines virtuelles et avec les opérations de centres de données virtuels. Ce livre suppose aussi que vous connaissez l'infrastructure VMware 5.x, notamment VMware ESX, vCenter Server et vSphere Client.

Vue générale de vShield 1

VMware® vShield est une suite de dispositifs virtuels de sécurité conçue pour l'intégration dans VMware vCenter Server et VMware ESX. vShield est un composant de sécurité essentiel pour protéger les centres de données virtualisés contre les attaques et les utilisations abusives et vous permettre d'atteindre vos objectifs de conformité réglementaires.

Ce guide suppose que vous avez un accès d'administrateur à la totalité du système vShield. Les ressources pouvant être affichées dans l'interface utilisateur de vShield Manager peuvent être différentes en fonction des rôles et droits attribués à un utilisateur ainsi que de la licence. Si vous ne pouvez pas accéder à un écran ou effectuer une tâche, consultez votre administrateur vShield.

- À propos des composants vShield page 9

  vShield inclut des composants et services essentiels pour la protection de vos machines virtuelles. vShield peut se configurer par une interface utilisateur web, un plug-in de vSphere Client, une interface de ligne de commande (CLI), et une API REST.

- Migration des composants vShield page 11

  Les dispositifs virtuels vShield Manager et vShield Edge peuvent être migrés automatiquement ou manuellement selon des stratégies DRS et HA. vShield Manager doit toujours être actif, vous devez donc migrer vShield Manager chaque fois que l'hôte ESX en cours doit subir un redémarrage ou une exploitation en mode maintenance.

- À propos de VMware Tools sur les composants vShield page 11

  Chaque dispositif virtuel de vShield inclut VMware Tools. Ne pas mettre à jour ni désinstaller la version de VMware Tools incluse avec un dispositif virtuel vShield.

- Ports nécessaires pour la communication vShield page 11

À propos des composants vShield

vShield inclut des composants et services essentiels pour la protection de vos machines virtuelles. vShield peut se configurer par une interface utilisateur web, un plug-in de vSphere Client, une interface de ligne de commande (CLI), et une API REST.

Pour lancer vShield, il vous faut une machine virtuelle vShield Manager et au moins un module vShield App ou vShield Edge.

vShield Manager

vShield Manager est le composant centralisé de gestion de réseau de vShield et s'installe comme machine virtuelle depuis un fichier OVA à l'aide de vSphere Client. Les administrateurs peuvent installer, configurer et gérer les composants vShield par l'interface utilisateur de vShield Manager. vShield Manager peut s'exécuter sur un hôte ESX différent de celui qui contient vos modules vShield App et vShield Edge.

vShield Manager tire parti du SDK VMware Infrastructure pour afficher une copie du panneau d'inventaire vSphere Client.

Pour en savoir plus sur l'utilisation de l'interface utilisateur vShield Manager, consultez Chapitre 2, « Bases de l'interface utilisateur de vShield Manager », page 13.

vShield Edge

vShield Edge fournit des services de sécurité de frontière et de passerelle pour isoler les machines virtuelles dans un groupe de ports, un groupe de ports vDS ou Cisco® Nexus 1000V. vShield Edge permet de connecter des réseaux isolés ou réseaux d'extrémité sur des réseaux partagés (liaison montante) en fournissant des services communs de passerelle tels que DHCP, VPN, NAT, et équilibrage de charge. Les déploiements courants de vShield Edge s'effectuent notamment dans la DMZ, les extranets de VPN et des environnements de Cloud à plusieurs partenaires où vShield Edge assure la sécurité périmétrique pour les centres de données virtuels (VDC).

Remarque Vous devez obtenir une licence d'évaluation ou complète pour utiliser vShield Edge.

Services standard vShield Edge (y compris vCloud Director)

- Pare-feu : Les règles prises en charge sont notamment la configuration IP 5-tuple avec plages d'adresses IP et de ports pour l'inspection d'état des protocoles TCP, UDP et ICMP.
- Traduction d'adresse réseau : Contrôles séparés des adresses IP source et destination, ainsi que traduction de ports TCP et UDP.
- Protocole DHCP (Dynamic Host Configuration Protocol) : Configuration de pools d'adresses IP, de passerelles, de serveurs DNS et des domaines de recherche.

Services avancés vShield Edge

- Réseau privé virtuel (VPN) d'un site à l'autre : Utilise les paramètres de protocole standardisé IPsec pour l'interopérabilité avec les grands fabricants de pare-feu.
- Équilibrage de charge : Adresses IP et groupes de serveurs virtuels configurables de façon simple et dynamique.

vShield Edge autorise l'exportation syslog de tous les services vers des serveurs distants.

vShield App

vShield App est un pare-feu intérieur au niveau de la carte réseau virtuelle permettant de créer des stratégies de contrôle d'accès indépendamment de la topologie du réseau. vShield App surveille tout le trafic entrant et sortant d'un hôte ESX, notamment entre les machines virtuelles dans le même groupe de ports. vShield App inclut l'analyse de trafic et la création de stratégies en fonction du conteneur.

vShield App installe un module hyperviseur et un dispositif virtuel de service de pare-feu. vShield App s'intègre avec les hôtes ESX grâce aux API VMsafe et collabore avec les fonctionnalités de la plate-forme VMware vSphere telles que DRS, vMotion, DPM et le mode de maintenance.

vShield App assure la protection par pare-feu entre les machines virtuelles en insérant un filtre de pare-feu sur chaque carte réseau virtuelle. Le filtre du pare-feu est transparent et n'exige pas de modification du réseau ni d'adresses IP pour créer des zones de sécurité. Vous pouvez écrire des règles d'accès à partir de conteneurs vCenter, comme des centres de données, clusters, pools de ressources et vApps, ou d'objets réseau tels que des groupes de ports et des VLAN, pour réduire le nombre de règles de pare-feu et faciliter le suivi de ces règles.

Vous devez installer des instances de vShield App sur tous les hôtes ESX d'un cluster pour protéger l'exploitation de VMware vMotion™ et des machines virtuelles lors de leur migration entre hôtes ESX. Par défaut, un dispositif virtuel vShield App ne peut pas être déplacé à l'aide de vMotion.

La fonctionnalité Flow Monitoring affiche les flux réseau autorisés et bloqués au niveau du protocole d'application. Vous pouvez utiliser ces informations pour effectuer un audit du trafic réseau et un dépannage opérationnel.

Remarque Vous devez obtenir une licence d'évaluation ou complète pour utiliser vShield App.

vShield Endpoint

vShield Endpoint transfère le traitement des agents antivirus et contre les logiciels malveillants vers un dispositif virtuel sécurisé et dédié, fourni par des partenaires VMware. Étant donné que le dispositif virtuel sécurisé (à la différence d'une machine virtuelle cliente) n'est pas déconnecté, il peut mettre à jour en permanence les signatures antivirus, assurant ainsi une protection ininterrompue des machines virtuelles sur l'hôte. Par ailleurs, les nouvelles machines virtuelles (ou les machines virtuelles existantes qui ont été déconnectées) sont protégées immédiatement contre la plupart des signatures antivirus actuelles lorsqu'elles sont connectées.

vShield Endpoint installe un module hyperviseur et un dispositif virtuel de sécurité d'un fournisseur antivirus tiers (partenaires VMware) sur un hôte ESX.

Remarque Vous devez obtenir une licence d'évaluation ou complète pour utiliser vShield Endpoint.

vShield Data Security

vShield Data Security offre une visibilité dans les données sensibles stockées dans les environnements virtualisés et de nuage de votre organisation. Selon les violations signalées par vShield Data Security, vous pouvez garantir que les données sensibles sont protégées de manière adéquate et évaluer la conformité aux réglementations mondiales.

Migration des composants vShield

Les dispositifs virtuels vShield Manager et vShield Edge peuvent être migrés automatiquement ou manuellement selon des stratégies DRS et HA. vShield Manager doit toujours être actif, vous devez donc migrer vShield Manager chaque fois que l'hôte ESX en cours doit subir un redémarrage ou une exploitation en mode maintenance.

Chaque vShield Edge doit être déplacé avec son groupe de ports sécurisé pour maintenir les paramètres et services de sécurité.

vShield App, vShield Endpoint ou vShield Data Security ne peuvent pas être transférés vers un autre hôte ESX. Si l'hôte ESX sur lequel résident ces composants nécessite un fonctionnement en mode de maintenance manuelle, vous devez décocher la case **[Move powered off and suspended virtual machines to other hosts in the cluster]** pour vous assurer que ces dispositifs virtuels ne soient pas migrés. Ces services redémarrent après la remise en ligne de l'hôte ESX.

À propos de VMware Tools sur les composants vShield

Chaque dispositif virtuel de vShield inclut VMware Tools. Ne pas mettre à jour ni désinstaller la version de VMware Tools incluse avec un dispositif virtuel vShield.

Ports nécessaires pour la communication vShield

vShield Manager nécessite l'ouverture des ports suivants :

- Accès aux ports ESX : 902/TCP et 903/TCP
- API REST : 80/TCP et 443/TCP

- Interface utilisateur graphique : 80/TCP à 443/TCP et initiations de connexions avec le SDK vSphere vCenter.
- Accès SSH à la ligne de commande CLI (non activé par défaut) : 22/TCP

Bases de l'interface utilisateur de vShield Manager 2

L'interface utilisateur vShield Manager propose des options de configuration et de consultation de données spécifiques de l'utilisation de vShield. Grâce au SDK VMware Infrastructure, vShield Manager affiche votre panneau d'inventaire vSphere Client pour une vue complète de votre environnement vCenter.

Remarque Vous pouvez enregistrer vShield Manager comme plug-in de vSphere Client. Ceci permet de configurer les composants de vShield depuis vSphere Client. Pour en savoir plus, consultez « Enregistrer vShield Manager comme plug-in vSphere Client », page 18.

- Se connecter à l'interface utilisateur de vShield Manager page 13

  Vous pouvez accéder à l'interface de gestion de vShield Manager à l'aide d'un navigateur web.

- À propos de l'interface utilisateur de vShield Manager page 14

  L'interface utilisateur de vShield Manager se divise en deux panneaux : le panneau d'inventaire et le panneau de configuration. Vous pouvez sélectionner une vue et une ressource sur le panneau d'inventaire pour ouvrir les détails et options de configuration disponibles dans le panneau de configuration.

Se connecter à l'interface utilisateur de vShield Manager

Vous pouvez accéder à l'interface de gestion de vShield Manager à l'aide d'un navigateur web.

Procédure

1 Ouvrez une fenêtre de navigateur web et tapez l'adresse IP attribuée à vShield Manager.

L'interface utilisateur vShield Manager s'ouvre dans une session SSL/HTTPS (ou ouvre une session SSL sécurisée).

2 Acceptez le certificat de sécurité.

Remarque Pour utiliser un certificat SSL pour l'authentification, consultez « Ajouter un certificat SSL pour identifier le service Web vShield Manager », page 20.

L'écran de connexion vShield Manager apparaît.

3 Connectez-vous à l'interface utilisateur vShield Manager à l'aide du nom d'utilisateur **`admin`** et du mot de passe **`default`**.

Vous devriez changer le mot de passe dès que possible pour éviter toute utilisation non autorisée. Reportez-vous à la section « Modifier un compte d'utilisateur », page 23.

4 Cliquez sur **[Log In]** .

À propos de l'interface utilisateur de vShield Manager

L'interface utilisateur de vShield Manager se divise en deux panneaux : le panneau d'inventaire et le panneau de configuration. Vous pouvez sélectionner une vue et une ressource sur le panneau d'inventaire pour ouvrir les détails et options de configuration disponibles dans le panneau de configuration.

Un clic sur chaque objet d'inventaire fait apparaître un ensemble d'onglets spécifiques dans le panneau de configuration.

- Panneau d'inventaire de vShield Manager page 14

  La hiérarchie du panneau d'inventaire vShield Manager reprend celle de l'inventaire de vSphere Client.

- Panneau de configuration de vShield Manager page 15

  Le panneau de configuration vShield Manager présente les paramètres pouvant être configurés en fonction de la ressource d'inventaire sélectionnée ainsi que le résultat de l'opération vShield. Chaque ressource propose plusieurs onglets, chacun présentant des formulaires d'information ou de configuration correspondant à la ressource.

Panneau d'inventaire de vShield Manager

La hiérarchie du panneau d'inventaire vShield Manager reprend celle de l'inventaire de vSphere Client.

Les ressources incluent le dossier racine, les centres de données, les clusters, les groupes de ports, les hôtes ESX et les machines virtuelles . En conséquence, vShield Manager est solidaire de votre inventaire vCenter Server pour présenter une vue complète de votre déploiement virtuel. vShield Manager est la seule machine virtuelle qui n'apparaît pas dans le panneau d'inventaire vShield Manager. Les paramètres de vShield Manager se configurent depuis la ressource **[Settings & Reports]** en haut du panneau d'inventaire.

Le panneau d'inventaire propose plusieurs vues : Hosts & Clusters, Networks et Secured Port Groups. La vue Hosts & Clusters affiche les centres de données, clusters, pools de ressources et hôtes ESX de votre inventaire. La vue Networks affiche les réseaux VLAN et groupes de ports de votre inventaire. La vue Secured Port Groups affiche les groupes de ports protégés par les instances de vShield Edge. Les vues Hosts & Clusters et Networks sont cohérentes avec les vues correspondantes de vSphere Client.

Il existe des différences dans les icônes des machines virtuelles et des composants vShield entre les panneaux d'inventaire de vShield Manager et de vSphere Client. Les icônes personnalisées s'utilisent pour montrer la différence entre les composants vShield et les machines virtuelles, ainsi que les différences entre les machines virtuelles protégées et non protégées.

Tableau 2-1. Icônes de machine virtuelle vShield dans le panneau d'inventaire vShield Manager

Icône	Description
	Machine virtuelle sous tension protégée par un vShield App.
	Machine virtuelle sous tension non protégée par un vShield App.

- Actualisation du panneau d'inventaire page 15

  Pour actualiser la liste des ressources dans le panneau d'inventaire, cliquez sur . L'action d'actualisation demande à vCenter Server les dernières informations sur les ressources. Par défaut, vShield Manager demande les données sur les ressources à vCenter Server toutes les cinq minutes.

- Recherche dans le panneau d'inventaire page 15

  Pour rechercher une ressource dans le panneau d'inventaire, tapez une chaîne dans le champ situé au-dessus du panneau d'inventaire de vShield Manager et cliquez sur .

Actualisation du panneau d'inventaire

Pour actualiser la liste des ressources dans le panneau d'inventaire, cliquez sur . L'action d'actualisation demande à vCenter Server les dernières informations sur les ressources. Par défaut, vShield Manager demande les données sur les ressources à vCenter Server toutes les cinq minutes.

Recherche dans le panneau d'inventaire

Pour rechercher une ressource dans le panneau d'inventaire, tapez une chaîne dans le champ situé au-dessus du panneau d'inventaire de vShield Manager et cliquez sur .

Panneau de configuration de vShield Manager

Le panneau de configuration vShield Manager présente les paramètres pouvant être configurés en fonction de la ressource d'inventaire sélectionnée ainsi que le résultat de l'opération vShield. Chaque ressource propose plusieurs onglets, chacun présentant des formulaires d'information ou de configuration correspondant à la ressource.

Du fait que chaque ressource a un objectif différent, certains onglets sont spécifiques de certaines ressources. Certains onglets peuvent aussi avoir un deuxième niveau d'options.

Paramètres du système de gestion 3

vShield Manager a besoin de communiquer avec vCenter Server et certains services tels que DNS et NTP pour fournir les détails de votre inventaire VMware Infrastructure.

Ce chapitre aborde les rubriques suivantes :

- « Connexion à vCenter Server », page 17
- « Enregistrer vShield Manager comme plug-in vSphere Client », page 18
- « Identifier les services DNS », page 18
- « Régler la date et l'heure de vShield Manager », page 19
- « Télécharger les journaux du support technique de vShield », page 19
- « Afficher l'état de vShield Manager », page 19
- « Ajouter un certificat SSL pour identifier le service Web vShield Manager », page 20

Connexion à vCenter Server

La connexion à votre vCenter Server permet à vShield Manager d'afficher votre inventaire VMware Infrastructure.

Procédure

1 Connectez-vous à vShield Manager.

Lors de la connexion initiale, vShield Manager s'ouvre sur l'onglet **[Configuration > vCenter]** . Si vous n'avez pas configuré le formulaire de l'onglet **[vCenter]** , procédez comme suit :

a Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

b Cliquez sur l'onglet **[Configuration]** .

L'écran **[vCenter]** s'affiche.

2 Sous vCenter Server Information, tapez l'adresse IP de vCenter Server dans le champ **[Server IP Address/Name]** .

3 Tapez votre nom d'utilisateur de connexion vSphere Client dans le champ **[Administrator User Name]** .

Le compte d'utilisateur doit disposer d'un accès administrateur.

4 Tapez le mot de passe associé à ce nom d'utilisateur dans le champ **[Password]** .

5 Cliquez sur **[Save]** .

vShield Manager se connecte à vCenter Server, ouvre une session et utilise le SDK VMware Infrastructure pour remplir le panneau d'inventaire vShield Manager. Le panneau d'inventaire est présenté à gauche de l'écran. Cette arborescence de ressources doit correspondre à votre panneau d'inventaire VMware Infrastructure. vShield Manager n'apparaît pas dans le panneau d'inventaire vShield Manager.

Enregistrer vShield Manager comme plug-in vSphere Client

L'option plug-in vSphere permet d'enregistrer vShield Manager comme plug-in de vSphere Client. Après enregistrement du plug-in, vous pouvez ouvrir l'interface utilisateur de vShield Manager depuis vSphere Client.

Procédure

1 Si vous êtes connecté à vSphere Client, déconnectez-vous.

2 Connectez-vous à vShield Manager.

3 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

4 Cliquez sur l'onglet **[Configuration]** .

L'écran **[vCenter]** s'affiche.

5 Sous **[vSphere Plug-in]** , cliquez sur **[Enregistrer]** .

L'enregistrement peut prendre quelques minutes.

6 Connectez-vous à vSphere Client.

7 Sélectionnez un hôte ESX.

8 Vérifiez que **[vShield]** apparaît comme onglet.

Suivant

Vous pouvez installer et configurer des composants de vShield depuis vSphere Client.

Identifier les services DNS

Vous devez spécifier au moins un serveur DNS lors de l'installation de vShield Manager. Les serveurs DNS spécifiés apparaissent dans l'interface utilisateur de vShield Manager.

Dans l'interface utilisateur de vShield Manager, vous pouvez spécifier jusqu'à trois serveurs DNS que vShield Manager pourra utiliser pour la résolution d'adresses IP et de noms d'hôte.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

L'écran **[vCenter]** s'affiche.

3 Sous **[DNS Servers]** , tapez une adresse IP dans **[Primary DNS IP Address]** pour identifier le serveur DNS primaire.

Ce serveur sera consulté en premier pour toutes les demandes de résolution.

4 (Facultatif) Tapez une adresse IP dans le champ **[Secondary DNS IP Address]** .

5 (Facultatif) Tapez une adresse IP dans le champ **[Tertiary DNS IP Address]** .

6 Cliquez sur **[Save]** .

Régler la date et l'heure de vShield Manager

Vous pouvez définir la date, l'heure et le fuseau horaire de vShield Manager pour horodater les événements et les données. Vous pouvez aussi spécifier une connexion à un serveur NTP pour définir une heure commune sur le réseau.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Date/Time]** .

4 Dans le champ **[Date and Clock]** , tapez la date et l'heure au format `YYYY-MM-DD HH:MM:SS`.

5 Dans le champ **[NTP Server]** , tapez l'adresse IP de votre serveur NTP.

Vous pouvez taper le nom d'hôte de votre serveur NTP si vous avez configuré un service DNS.

6 Dans le menu déroulant **[Time Zone]** , sélectionnez le fuseau horaire approprié.

7 Cliquez sur **[Save]** .

Télécharger les journaux du support technique de vShield

Vous pouvez télécharger le journal système depuis un composant vShield vers votre PC. Un journal système peut être utilisé pour résoudre les problèmes de fonctionnement.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Support]** .

4 Sous **[Tech Support Log Download]** , cliquez sur **[Initiate]** en regard du composant approprié.

Après cette initiation, le journal est généré et envoyé à vShield Manager. Ceci peut prendre quelques secondes.

5 Dès que le journal est prêt, cliquez sur le lien **[Download]** pour télécharger le journal vers votre PC.

Le journal est compressé et il porte l'extension `.gz`.

Suivant

Vous pouvez ouvrir le journal à l'aide d'un utilitaire de décompression en recherchant **[All Files]** dans le répertoire où vous avez enregistré le fichier.

Afficher l'état de vShield Manager

vShield Manager affiche l'utilisation des ressources système.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Status]** .

Suivant

Reportez-vous à la section « Afficher le logiciel système en cours », page 25.

Ajouter un certificat SSL pour identifier le service Web vShield Manager

Vous pouvez générer ou importer un certificat SSL dans vShield Manager pour authentifier l'identité u service web vShield Manager et chiffrer les données envoyées au serveur web vShield Manager. Une bonne pratique de sécurité consiste à utiliser l'option de génération de certificat pour générer une clé privée et une clé publique, et enregistrer la clé privée dans vShield Manager.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[SSL Certificate]** .

4 Sous **[Generate Certificate Signing Request]** , remplissez le formulaire en complétant les champs suivants :

Option	Action
[Common Name]	Entrez le nom correspondant au site. Par exemple, si l'adresse IP de l'interface de gestion de vShield Manager est 192.168.1.10, entrez **`192.168.1.10`**.
[Organization Unit]	Entrez le service de la société qui commande le certificat.
[Organization Name]	Entrez le nom juridique complet de votre société.
[City Name]	Entrez le nom complet de la ville où se trouve votre société.
[State Name]	Entrez le nom complet de l'état où se trouve votre société.
[Country Code]	Entrez le code à deux chiffres représentant votre pays. Par exemple, les États-Unis sont **US** et la France FR.
[Key Algorithm]	Sélectionnez l'algorithme cryptographique à utiliser : DSA ou RSA.
[Key Size]	Sélectionnez le nombre de bits utilisés dans l'algorithme sélectionné.

5 Cliquez sur **[Generate]** .

Importer un certificat SSL

Vous pouvez importer un certificat SSL préexistant pour l'utiliser avec vShield Manager.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[SSL Certificate]** .

4 Sous Import Signed Certificate, cliquez sur **[Browse]** en regard de Certificate File pour trouver le fichier.

5 Sélectionnez le type de fichier certificat dans la liste déroulante **[Certificate Type]** .

6 Cliquez sur **[Apply]** .

Le certificat est stocké dans vShield Manager.

Gestion d'utilisateurs 4

Les opérations de sécurité peuvent être gérées par plusieurs personnes. La gestion de la totalité du système est déléguée à des personnes différentes en fonction de catégories logiques. Mais les autorisations d'effectuer certaines tâches doivent être limitées aux seuls utilisateurs disposant des droits appropriés sur des ressources spécifiques. La section Users permet de déléguer cette gestion des ressources aux utilisateurs en leur attribuant des droits appropriés.

La gestion d'utilisateurs dans l'interface utilisateur de vShield Manager est séparée de la gestion d'utilisateurs dans la ligne de commande CLI de tout composant vShield.

Ce chapitre aborde les rubriques suivantes :

- « Gestion des comptes d'utilisateur », page 21
- « Gestion du compte d'utilisateur par défaut », page 22
- « Ajouter un compte d'utilisateur », page 22
- « Modifier un compte d'utilisateur », page 23
- « Changer un rôle d'utilisateur », page 24
- « Désactiver ou activer un compte d'utilisateur », page 24
- « Supprimer un compte d'utilisateur », page 24

Gestion des comptes d'utilisateur

Dans l'interface utilisateur vShield Manager, le rôle d'un utilisateur définit les actions que cet utilisateur est autorisé à effectuer sur une ressource donnée. Le rôle détermine les activités autorisées de l'utilisateur sur une ressource donnée, pour s'assurer que chaque utilisateur n'a accès qu'aux fonctions nécessaires pour effectuer les opérations applicables. Cela autorise un contrôle de domaine sur des ressources spécifiques ou sur l'ensemble du système si votre autorisation n'a pas de restrictions.

Les règles suivantes sont appliquées :

- Un utilisateur ne peut avoir qu'un seul rôle.
- Vous ne pouvez pas ajouter un rôle à un utilisateur ni supprimer un rôle affecté à un utilisateur. Toutefois, vous pouvez changer le rôle affecté à l'utilisateur.

Tableau 4-1. Rôles d'utilisateur vShield Manager

Droit	Autorisations
Enterprise Administrator	Opérations et sécurité vShield
vShield Administrator	Opérations vShield uniquement : par exemple, installation de dispositifs virtuels, configuration de groupes de ports.

Tableau 4-1. Rôles d'utilisateur vShield Manager (suite)

Droit	Autorisations
Security Administrator	Sécurité vShield uniquement : par exemple, définition de stratégie de sécurité des données, création de groupes de ports, création de rapports pour les modules vShield.
Auditor	Lecture uniquement.

L'étendue d'un rôle détermine les ressources que peut voir un utilisateur. Les étendues suivantes sont disponibles pour les utilisateurs vShield.

Tableau 4-2. Portée d'utilisateur vShield Manager

Portée	Description
Aucune restriction	Accès à la totalité du système vShield
Limite l'étendue d'accès aux groupes de ports sélectionnés ci-dessous	Accès à un centre de données ou à un groupe de ports donné

Les rôles Enterprise Administrator et vShield Administrator peuvent être affectés uniquement aux utilisateurs vCenter et leur étendue d'accès est globale (aucune restriction).

Gestion du compte d'utilisateur par défaut

L'interface utilisateur vShield Manager contient un compted'utilisateur local qui dispose de droits d'accès à toutes les ressources. Vous ne pouvez pas modifier les droits ni supprimer cet utilisateur. Le nom d'utilisateur par défaut est **`admin`** et le mot de passe par défaut est **`default`**.

Changez le mot de passe de ce compte à la connexion initiale avec vShield Manager. Reportez-vous à la section « Modifier un compte d'utilisateur », page 23.

Ajouter un compte d'utilisateur

Vous pouvez créer un utilisateur local pour vShield ou affecter un rôle à un utilisateur vCenter. Lorsque vous affectez un rôle à un utilisateur vCenter, vCenter authentifie le rôle avec Active Directory.

Créer un utilisateur local

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Users]** .

3 Cliquez sur **[Add]** .

La fenêtre Assign Role s'affiche.

4 Cliquez sur **[Create a new user local to vShield]** .

5 Tapez une adresse **[Email]** .

6 Tapez un **[Login ID]** .

Ce nom permettra la connexion à l'interface utilisateur de vShield Manager. Ce nom d'utilisateur et le mot de passe associé ne peuvent pas être utilisés pour accéder aux lignes de commande CLI de vShield App ou de vShield Manager.

7 Tapez le **[Full Name]** de l'utilisateur à des fins d'identification.

8 Tapez dans **[Password]** un mot de passe de connexion.

9 Retapez le mot de passe dans le champ **[Retype Password]** .

10 Cliquez sur **[Next]** .

11 Sélectionnez le rôle de l'utilisateur et cliquez sur **[Next]** . Pour plus d'informations sur les rôles disponibles, voir « Gestion des comptes d'utilisateur », page 21.

12 Sélectionnez la portée de l'utilisateur et cliquez sur **[Finish]** .

Le compte d'utilisateur apparaît dans la table Users.

Affecter un rôle à un utilisateur vCenter

Lorsque vous affectez un rôle à un utilisateur vCenter, vCenter authentifie le rôle avec Active Directory.

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Users]** .

3 Cliquez sur **[Add]** .

La fenêtre Assign Role s'affiche.

4 Cliquez sur **[Select vCenter user]** .

5 Tapez le nom de l' **[User]** vCenter.

REMARQUE Si l'utilisateur vCenter appartient à un domaine, vous devez entrer un chemin de domaine Windows qualifié complet. Ce nom d'utilisateur est utilisé pour la connexion à l'interface utilisateur vShield Manager et il ne peut pas l'être pour accéder aux interfaces CLI vShield App et vShield Manager.

---

6 Cliquez sur **[Next]** .

7 Sélectionnez le rôle de l'utilisateur et cliquez sur **[Next]** . Pour plus d'informations sur les rôles disponibles, voir « Gestion des comptes d'utilisateur », page 21.

8 Sélectionnez la portée de l'utilisateur et cliquez sur **[Finish]** .

Le compte d'utilisateur apparaît dans la table Users.

Modifier un compte d'utilisateur

Vous pouvez modifier un compte d'utilisateur pour changer le mot de passe, le rôle et la portée. Vous ne pouvez pas modifier le compte **`admin`**.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Users]** .

3 Sélectionnez l'utilisateur à modifier.

4 Cliquez sur **[Edit]** .

5 Effectuez les modifications nécessaires.

Si vous changez le mot de passe, confirmez-le en le tapant une deuxième fois dans le champ **[Retype Password]** .

6 Cliquez sur **[Finish]** pour enregistrer vos modifications.

Changer un rôle d'utilisateur

Vous pouvez changer l'affectation de rôle de tous les utilisateurs, sauf celui de l'utilisateur **admin**.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Users]** .

3 Sélectionnez l'utilisateur dont vous voulez changer le rôle.

4 Cliquez sur **[Change Role]** .

5 Effectuez les modifications nécessaires.

6 Cliquez sur **[Finish]** pour enregistrer vos modifications.

Désactiver ou activer un compte d'utilisateur

Vous pouvez désactiver un compte d'utilisateur pour empêcher l'utilisateur de se connecter à vShield Manager. Vous ne pouvez pas désactiver l'utilisateur **admin**.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Users]** .

3 Sélectionnez un compte d'utilisateur.

4 Effectuez l'une des opérations suivantes.

- Cliquez sur **[Actions] > [Disable selected user(s)]** pour désactiver un compte d'utilisateur.
- Cliquez sur **[Actions] > [Enable selected user(s)]** pour activer un compte d'utilisateur.

Supprimer un compte d'utilisateur

Vous pouvez supprimer tout compte d'utilisateur créé. Vous ne pouvez pas supprimer le compte d'utilisateur **admin**. Des enregistrements d'audit sont conservés dans la base de données pour les utilisateurs supprimés et peuvent être inclus dans un rapport de journal d'audit.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Users]** .

3 Sélectionnez l'utilisateur à supprimer.

4 Cliquez sur **[Delete]** .

5 Cliquez sur **[OK]** pour confirmer la suppression.

Si vous supprimez un compte d'utilisateur vCenter, seule l'affectation de rôle de vShield Manager est supprimée. Le compte d'utilisateur n'est pas supprimé dans vCenter.

Mise à jour du logiciel système 5

Le logiciel vShield nécessite des mises à jour périodiques pour conserver les performances du système. Les options de l'onglet **[Updates]** permettent d'installer et suivre les mises à jour du système.

- Afficher le logiciel système en cours page 25

  Vous pouvez afficher les versions installées du logiciel des composants vShield ou vérifier si une mise à jour est en cours.

- Envoyer une mise à jour page 25

  Les mises à jour de vShield sont disponibles hors ligne. Quand une mise à jour est rendue disponible, vous pouvez la télécharger sur votre PC, puis envoyer la mise à jour par l'interface utilisateur de vShield Manager.

Afficher le logiciel système en cours

Vous pouvez afficher les versions installées du logiciel des composants vShield ou vérifier si une mise à jour est en cours.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Updates]** .

3 Cliquez sur **[Update Status]** .

Envoyer une mise à jour

Les mises à jour de vShield sont disponibles hors ligne. Quand une mise à jour est rendue disponible, vous pouvez la télécharger sur votre PC, puis envoyer la mise à jour par l'interface utilisateur de vShield Manager.

Lors de l'envoi de la mise à jour, vShield Manager est mis à jour d'abord et chaque vShield Zones ou vShield App est mis à jour ensuite. Si un redémarrage de vShield Manager ou d'un vShield Zones ou App est nécessaire, l'écran **[Update Status]** vous invite à redémarrer le composant. Si vShield Manager et toutes les instances vShield Zones et vShield App doivent être redémarrées, vous devez redémarrer vShield Manager d'abord, puis redémarrer chaque vShield Zones ou App.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Updates]** .

3 Cliquez sur **[Upload Upgrade Bundle]** .

4 Cliquez sur **[Browse]** pour trouver la mise à jour.

5 Quand vous avez trouvé le fichier, cliquez sur **[Upload File]** .

6 Cliquez sur **[Update Status]** puis cliquez sur **[Install]** .

7 Cliquez sur **[Confirm Install]** pour confirmer l'installation de la mise à jour.

Il y a deux tableaux sur cet écran. Pendant l'installation, vous pouvez consulter la table du haut qui contient la description, l'heure de début, l'état de réussite et l'état de traitement de la mise à jour en cours. Consultez la table du bas pour l'état de mise à jour de chaque vShield App. Toutes les instances de vShield App ont été mises à niveau quand l'état de la dernière vShield App est affichée comme **[Finished]** .

8 Après le redémarrage de vShield Manager, cliquez sur l'onglet **[Update Status]** .

9 Cliquez sur **[Reboot Manager]** si vous y êtes invité.

10 Cliquez sur **[Finish Install]** pour terminer la mise à jour du système.

11 Cliquez sur **[Confirm]** .

Sauvegarde des données de vShield Manager 6

Vous pouvez sauvegarder et restaurer vos données de vShield Manager, ce qui peut inclure la configuration du système, les événements et les tables de journaux d'audit. Les tables de configuration sont incluses dans chaque sauvegarde. Mais vous pouvez exclure les événements système et de journal d'audit. Les sauvegardes sont enregistrées à un emplacement distant qui doit être accessible à vShield Manager.

Les sauvegardes peuvent être exécutées selon un programme ou sur demande.

- Sauvegarde sur demande de vos données vShield Manager page 27

  Vous pouvez sauvegarder vos données vShield Manager à tout moment par une sauvegarde sur demande.

- Programmer une sauvegarde des données de vShield Manager page 28

  Vous ne pouvez programmer les paramètres que d'un seul type de sauvegarde à la fois. Vous ne pouvez pas programmer une sauvegarde de configuration seulement et une sauvegarde complète des données pour exécution simultanée.

- Restaurer une sauvegarde page 29

  Vous pouvez restaurer un sauvegarde uniquement sur une machine virtuelle qui vient d'être déployée.

Sauvegarde sur demande de vos données vShield Manager

Vous pouvez sauvegarder vos données vShield Manager à tout moment par une sauvegarde sur demande.

Procédure

1. Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.
2. Cliquez sur l'onglet **[Configuration]** .
3. Cliquez sur **[Backups]** .
4. (Facultatif) Cochez la case **[Exclude System Events]** pour ne pas sauvegarder les tables d'événements système.
5. (Facultatif) Cochez la case **[Exclude Audit Logs]** pour ne pas sauvegarder les tables de journal d'audit.
6. Tapez dans **[Host IP Address]** l'adresse IP du système sur lequel la sauvegarde sera enregistrée.
7. Tapez le **[Host Name]** du système de sauvegarde.
8. Tapez dans **[User Name]** le nom d'utilisateur nécessaire pour se connecter au système de sauvegarde.
9. Tapez dans **[Password]** le mot de passe associé au nom d'utilisateur pour le système de sauvegarde.
10. Dans le champ **[Backup Directory]** , tapez le chemin absolu d'enregistrement des sauvegardes.

11 Tapez une chaîne de texte dans **[Filename Prefix]** .

Ce texte sera ajouté devant le nom de fichier de la sauvegarde pour faciliter la reconnaissance sur le système de sauvegarde. Si vous tapez par exemple **ppdb**, la sauvegarde résultante sera nommée `ppdbHH_MM_SS_JourJJMoiAAAA`.

12 Entrez une **[Pass Phrase]** pour protéger le fichier de sauvegarde.

13 Sur le menu déroulant **[Transfer Protocol]** , sélectionnez **[SFTP]** ou **[FTP]** .

14 Cliquez sur **[Backup]** .

Une fois terminée, la sauvegarde apparaît dans une table sous ce formulaire.

15 Cliquez sur **[Save Settings]** pour enregistrer la configuration.

Programmer une sauvegarde des données de vShield Manager

Vous ne pouvez programmer les paramètres que d'un seul type de sauvegarde à la fois. Vous ne pouvez pas programmer une sauvegarde de configuration seulement et une sauvegarde complète des données pour exécution simultanée.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Backups]** .

4 Sur le menu de la liste déroulante **[Scheduled Backups]** , sélectionnez **[On]** .

5 Sur le menu déroulant **[Backup Frequency]** , sélectionnez **[Hourly]** , **[Daily]** ou **[Weekly]** .

Les menus **[Day of Week]** , **[Hour of Day]** et **[Minute]** sont désactivés en fonction de la fréquence sélectionnée. Si vous sélectionnez par exemple **[Daily]** , le menu déroulant **[Day of Week]** est désactivé car ce champ n'est pas applicable à une fréquence quotidienne.

6 (Facultatif) Cochez la case **[Exclude System Events]** pour ne pas sauvegarder les tables d'événements système.

7 (Facultatif) Cochez la case **[Exclude Audit Log]** pour ne pas sauvegarder les tables des journaux d'audit.

8 Tapez dans **[Host IP Address]** l'adresse IP du système sur lequel la sauvegarde sera enregistrée.

9 (Facultatif) Tapez le **[Host Name]** du système de sauvegarde.

10 Tapez dans **[User Name]** le nom d'utilisateur nécessaire pour se connecter au système de sauvegarde.

11 Tapez dans **[Password]** le mot de passe associé au nom d'utilisateur pour le système de sauvegarde.

12 Dans le champ **[Backup Directory]** , tapez le chemin absolu d'enregistrement des sauvegardes.

13 Tapez une chaîne de texte dans **[Filename Prefix]** .

Ce texte sera ajouté devant chaque nom de fichier de la sauvegarde pour faciliter la reconnaissance sur le système de sauvegarde. Si vous tapez par exemple **ppdb**, la sauvegarde résultante sera nommée `ppdbHH_MM_SS_JourJJMoiAAAA`.

14 Dans le menu déroulant **[Transfer Protocol]** , sélectionnez **[SFTP]** ou **[FTP]** , selon ce que la destination prend en charge.

15 Cliquez sur **[Save Settings]** .

Restaurer une sauvegarde

Vous pouvez restaurer un sauvegarde uniquement sur une machine virtuelle qui vient d'être déployée.

Pour restaurer une sauvegarde disponible, les champs **[Host IP Address]** , **[User Name]** , **[Password]** et **[Backup Directory]** de l'écran **[Backups]** doivent avoir des valeurs permettant de désigner l'emplacement de la sauvegarde à restaurer. Si le fichier de sauvegarde contient des données d'événement système et de journal d'audit, ces données sont aussi restaurées.

IMPORTANT Sauvegardez vos données en cours avant de restaurer un fichier de sauvegarde.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Configuration]** .

3 Cliquez sur **[Backups]** .

4 Cliquez sur **[View Backups]** pour afficher toutes les sauvegardes disponibles enregistrées sur le serveur de sauvegarde.

5 Cochez la case correspondant à la sauvegarde à restaurer.

6 Cliquez sur **[Restore]** .

7 Cliquez sur **[OK]** pour confirmer.

Événements système et journaux d'audit 7

Les événements système sont des événements associés au fonctionnement de vShield. Ils sont signalés pour détailler chaque événement d'exploitation, par exemple un redémarrage de vShield App ou une rupture de communication entre vShield App et vShield Manager. Les événements peuvent concerner l'exploitation de base (type Informational) ou une erreur critique (Critical).

Ce chapitre aborde les rubriques suivantes :

- « Afficher le rapport d'événements système », page 31
- « Événements de dispositif virtuel vShield Manager », page 31
- « Événements vShield App », page 32
- « À propos du format Syslog », page 33
- « Afficher le journal d'audit », page 33

Afficher le rapport d'événements système

vShield Manager place les événements système dans un rapport que vous pouvez filtrer en fonction de la vShield App et de la gravité des événements.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[System Events]** .

3 (Facultatif) Sélectionnez une ou plusieurs instances vShield App dans le champ **[vShield]** .

Toutes les instances vShield App sont sélectionnées par défaut.

4 Dans le menu déroulant **[and Severity]** , sélectionnez la gravité à utiliser pour filtrer les résultats.

Toutes les gravités sont incluses par défaut. Vous pouvez sélectionner une ou plusieurs gravités simultanément.

5 Cliquez sur **[View Report]** .

6 Dans le rapport généré, cliquez sur le lien **[Event Time]** pour afficher des informations sur un événement donné.

Événements de dispositif virtuel vShield Manager

Les événements suivants sont spécifiques au dispositif virtuel vShield Manager.

Tableau 7-1. Événements de dispositif virtuel vShield Manager

	Mise hors tension	Mise sous tension	Activation d'interface	Désactivation d'interface
CLI locale	Lancez la commande `show log follow`.	Lancez la commande `show log follow`.	Lancez la commande `show log follow`.	Lancez la commande `show log follow`.
Interface utilisateur	ND	ND	ND	ND

Tableau 7-2. Événements de dispositif virtuel vShield Manager

	CPU	Mémoire	Stockage
CLI locale	Lancez la commande `show process monitor`.	Lancez la commande `show system memory`.	Lancez la commande `show filesystem`.
Interface utilisateur	Reportez-vous à la section « Afficher l'état de vShield Manager », page 19.	Reportez-vous à la section « Afficher l'état de vShield Manager », page 19.	Reportez-vous à la section « Afficher l'état de vShield Manager », page 19.

Événements vShield App

Les événements suivants sont spécifiques aux dispositifs virtuels vShield App.

Tableau 7-3. Événements vShield App

	Mise hors tension	Mise sous tension	Activation d'interface	Désactivation d'interface
CLI locale	Lancez la commande `show log follow`.	Lancez la commande `show log follow`.	Lancez la commande `show log follow`.	Lancez la commande `show log follow`.
Syslog	ND	Consultez « À propos du format Syslog », page 33	`e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex`. Pour l'écriture de script sur le serveur syslog, recherchez **`NIC Link is`**.	`e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex`. Pour l'écriture de script sur le serveur syslog, recherchez **`NIC Link is`**.
Interface utilisateur	Événement « Heartbeat failure » dans le journal des événements système. Consultez « Afficher le rapport d'événements système », page 31	Consultez « Affichage de l'état système en cours d'une vShield App », page 50	Consultez « Affichage de l'état système en cours d'une vShield App », page 50	Consultez « Affichage de l'état système en cours d'une vShield App », page 50

Tableau 7-4. Événements vShield App

	CPU	Mémoire	Stockage	Réinitialisation de session en raison d'un déni de service, d'inactivité ou de délai d'expiration des données
CLI locale	Lancez la commande `show process monitor`.	Lancez la commande `show system memory`.	Lancez la commande `show filesystem`.	Lancez la commande `show log follow`.
Syslog	ND	ND	ND	Consultez « À propos du format Syslog », page 33
Interface utilisateur	Consultez « Affichage de l'état système en cours d'une vShield App », page 50	Consultez « Affichage de l'état système en cours d'une vShield App », page 50	Consultez « Affichage de l'état système en cours d'une vShield App », page 50	Consultez le journal des événements système. Consultez « Afficher le rapport d'événements système », page 31

À propos du format Syslog

Le message d'événement système journalisé dans le syslog a la structure suivante :

```
en-tête syslog (horodatage + nom d'hôte + sysmgr/)
Horodatage (du service)
Paires nom/valeur
Le nom et la valeur sont séparés par le délimiteur '::' (double deux-points)
Chaque paire nom/valeur est séparé par le délimiteur ';;' (double point-virgule)
```

Les champs et les types de l'événement système contiennent les informations suivantes :

```
Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer (valeurs possibles : 10007 10016 10043 20019)
Severity :: string (valeurs possibles : INFORMATION LOW MEDIUM HIGH CRITICAL)
Message ::
```

Afficher le journal d'audit

L'onglet **[Audit Logs]** permet d'afficher les actions effectuées par tous les utilisateurs de vShield Manager. vShield Manager conserve les données de journal d'audit une année, ensuite les données sont abandonnées.

Procédure

1 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

2 Cliquez sur l'onglet **[Audit Logs]** .

3 Limitez les données en sortie en cliquant sur un ou plusieurs des filtres de colonne suivants :

Option	Action
[User Name]	Sélectionnez le nom de connexion d'un utilisateur qui a effectué l'action.
[Module]	Sélectionnez la ressource vShield sur laquelle l'action a été effectuée.
[Operation]	Sélectionnez le type d'action effectuée.

Option	Action
[Status]	Sélectionnez le résultat de l'action qui peut être Success ou Failure.
[Operation Span]	Sélectionnez le composant vShield sur lequel l'action a été effectuée. **[Local]** désigne vShield Manager.

Gestion de vShield Edge 8

vShield Edge fournit des services de sécurité de frontière et de passerelle pour isoler les machines virtuelles dans un groupe de ports, un groupe de ports vDS ou Cisco® Nexus 1000V. vShield Edge permet de connecter des réseaux isolés ou réseaux d'extrémité sur des réseaux partagés (liaison montante) en fournissant des services communs de passerelle tels que DHCP, VPN, NAT, et équilibrage de charge. Les déploiements courants de vShield Edge s'effectuent notamment dans la DMZ, les extranets de VPN et des environnements de Cloud à plusieurs partenaires où vShield Edge assure la sécurité périmétrique pour les centres de données virtuels (VDC).

Ce chapitre aborde les rubriques suivantes :

- « Afficher l'état d'un vShield Edge », page 35
- « Spécifier un serveur Syslog distant », page 36
- « Gestion du pare-feu vShield Edge », page 36
- « Gestion des règles NAT », page 40
- « Gestion du service DHCP », page 41
- « Gestion du service VPN », page 43
- « Ajouter une route statique. », page 45
- « Gérer le service d'équilibrage de charge », page 46
- « Démarrer ou arrêter les services vShield Edge », page 47
- « Redéployer vShield Edge », page 47

Afficher l'état d'un vShield Edge

L'option **[Status]** présente la configuration réseau et l'état des services d'un module vShield Edge. Les détails sont notamment l'adressage d'interface et l'ID réseau. Vous pouvez utiliser l'ID réseau pour envoyer des commandes d'API REST à un module vShield Edge.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

Spécifier un serveur Syslog distant

Vous pouvez envoyer les événements vShield Edge, par exemple infraction aux règles de pare-feu, vers un serveur syslog.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur **[Status]** .

5 Développez le panneau Remote Syslog Servers.

6 Cliquez sur **[Edit]** .

La boîte de dialogue Edit Syslog Servers Configuration s'affiche.

7 Tapez l'adresse IP d'un serveur syslog distant.

8 Cliquez sur **[OK]** pour enregistrer la configuration.

Gestion du pare-feu vShield Edge

vShield Edge assure une protection de pare-feu aux sessions entrantes et sortantes. La règle de pare-feu par défaut bloque tout le trafic entrant et autorise tout le trafic sortant. Outre la stratégie de pare-feu par défaut, vous pouvez configurer un ensemble de règles permettant d'autoriser ou de bloquer les sessions de trafic depuis et vers certaines sources et destinations précises. Vous pouvez gérer la stratégie de pare-feu par défaut comme l'ensemble de règles de pare-feu séparément pour chaque agent vShield Edge.

Lorsque vous mettez à niveau vShield Edge depuis une version antérieure, vShield Edge fonctionne en mode de compatibilité. Vous pouvez passer au mode normal.

En mode de compatibilité, la règle de pare-feu par défaut est appliquée uniquement sur l'interface interne. Tout le trafic dans les deux directions sur les interfaces externes et VPN est autorisé. Lorsque vous activez le mode normal, les règles de politique de pare-feu par défaut ne sont pas modifiées initialement. Lorsque vous changez la configuration du pare-feu, les règles de pare-feu par défaut de vShield Edge 5.0.1 sont appliquées lorsque le trafic entrant est bloqué et que le trafic sortant est autorisé.

Modifier les paramètres de pare-feu par défaut

Vous pouvez modifier les paramètres par défaut des règles de pare-feu. Les paramètres de pare-feu par défaut s'appliquent au trafic qui ne correspond à aucune règle de pare-feu.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur **[Firewall]** .

5 Dans le panneau **[Default Firewall Settings]** , cliquez sur **[Configure Settings]** .

La boîte de dialogue Edit Default Policy Configuration s'affiche.

6 Dans **[Default Traffic Policy]** , sélectionnez **[Block]** ou **[Allow]** . La valeur par défaut est **[Block]** .

7 Dans **[Default Policy Logging]** , sélectionnez **[Enable]** ou **[Disable]** . Si la journalisation est activée, les règles de pare-feu sont consignées dans les journaux vShield. Si un serveur syslog distant est configuré, les journaux s'affichent également sur le serveur syslog distant.

8 Dans **[ICMP Errors]** , cliquez sur **[Block]** ou **[Allow]** .

9 Cliquez sur **[OK]** .

Créer un groupe IP

Vous pouvez créer un groupe d'adresses IP constitué d'une plage d'adresse IP gb. Ensuite, vous pouvez ajouter ce groupe comme source ou destination dans une règle de pare-feu.

Procédure

1 Cliquez sur une ressource centre de données depuis vSphere Client.

2 Cliquez sur l'onglet **[vShield]** .

3 Cliquez sur l'onglet **[Grouping]** .

4 Cliquez sur **[Add]** et sélectionnez **[IP Addresses]** .

La fenêtre Ajouter des adresses IP s'affiche.

5 Tapez le nom du groupe d'adresses.

6 Tapez la description du groupe d'adresses.

7 Tapez les adresses IP à inclure dans le groupe.

8 Cliquez sur **[OK]** .

Créer une application

Tous les mappages personnalisés de paire application-port que vous avez définis dans un niveau précédent s'affichent comme applications par défaut.

Procédure

1 Dans vSphere Client, passez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données du panneau d'inventaire.

3 Cliquez sur l'onglet **[Applications]** .

4 Cliquez sur **[Add]** .

La fenêtre Add Application s'ouvre.

5 Tapez un **[Name]** pour identifier l'application.

6 (Facultatif) Tapez la **[Description]** de l'application.

7 (Facultatif) Sélectionnez le **[Protocol]** auquel vous voulez ajouter un port non standard.

8 Tapez le ou les numéros de port dans **[Ports]** =.

9 Cliquez sur **[Save]** .

L'application personnalisée apparaît dans la table Applications.

Ajouter une règle de pare-feu vShield Edge

Les règles de pare-feu vShield Edge régissent le trafic en fonction des critères suivants :

Tableau 8-1. Critère de règles de pare-feu vShield Edge

Critère	Description
[Source]	Adresse IP source de la communication.
[Source Port]	Port ou plage de ports d'origine de la communication. Pour entrer une plage de ports, séparez la valeur la plus basse et la valeur la plus haute de la plage par un tiret. Par exemple, 1000-1100.
[Destination]	Adresse IP visée par la communication.
[Traffic type]	Application ou protocole auquel s'applique la règle.
[Intf(Dir)]	Interface et direction de la transmission.
[Action]	Action à appliquer sur la transmission. Les options sont Allow ou Block. L'action par défaut sur tout le trafic entrant est Bloquer et tout le trafic sortant est Autoriser.
[Log]	Informations de trafic à consigner ou non.
[Enable]	La règle de pare-feu est activée ou désactivée.

Vous pouvez ajouter des plages de ports destination et source à une règle pour des services dynamiques tels que FTP et RPC, qui peuvent nécessiter plusieurs ports pour terminer une transmission. Si vous n'autorisez pas tous les ports qui doivent être ouverts pour une transmission, cette transmission est bloquée.

La règle de pare-feu par défaut autorise le trafic vers toutes les interfaces.

Tableau 8-2. Règle de pare-feu pour autoriser le trafic d'un réseau interne vers un serveur HTTP

Source	Source Port	Destination	Traffic type	Interface:Direction
192.168.0.0/24	Toutes	10.20.222.34	HTTP	Int:In

Tableau 8-3. Règle de pare-feu pour le trafic pour autoriser SSH dans une m/c dans un réseau interne

Source	Source Port	Destination	Traffic type	Interface:Direction
Toutes	Toutes	192.168.0.10	SSH	Sortie:Entrée

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Firewall]** .

5 Cliquez sur **[Add]** .

6 Dans **[Rule applied to]** , sélectionnez l'interface dans laquelle vous voulez ajouter la règle de pare-feu.

7 Sélectionnez la **[Traffic Direction]** à laquelle vous voulez appliquer la règle de pare-feu.

8 Dans **[Source]** , tapez l'adresse IP (ou le groupe d'adresses IP), la plage d'adresses IP ou le sous-réseau d'origine de la communication. Si vous ne sélectionnez pas cette option, vous indiquez que la règle s'applique au trafic depuis n'importe quelle source.

9 Dans **[Source Port]** , tapez le port ou la plage de ports d'origine de la communication.

10 Dans **[Destination]** , tapez l'adresse IP (ou le groupe d'adresses IP), la plage d'adresses IP ou le sous-réseau cible de la communication. Si vous ne sélectionnez pas cette option, vous indiquez que la règle s'applique au trafic depuis n'importe quelle destination.

11 Indiquez si le **[Type of traffic]** est une **[Known Application]** ou un **[Protocol]** . Sélectionnez l'application ou le protocole.

12 Dans **[Action]** , indiquez si vous voulez **[Block]** ou **[Allow]** le trafic.

13 Dans **[Rule]** , indiquez si vous voulez **[Enable]** ou **[Disable]** la règle que vous ajoutez.

14 Dans **[Logging]** , indiquez si vous voulez **[Log]** ou **[Do not log]** le trafic qui est alloué ou bloqué par la règle.

15 Tapez des **[Notes]** , si nécessaire.

16 Cliquez sur **[OK]** .

17 Cliquez sur **[Publish Changes]** .

Modifier une règle de pare-feu vShield Edge

Vous pouvez modifier n'importe quelle règle de pare-feu personnalisée.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Firewall]** .

5 Sélectionnez la règle à modifier.

6 Cliquez sur **[Edit Rule]** .

7 Modifiez les options appropriées.

8 Cliquez sur **[OK]** .

9 Cliquez sur **[Publish Changes]** .

Changer la priorité d'une règle de pare-feu vShield Edge

Vous pouvez changer la priorité des règles de pare-feu personnalisées.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Firewall]** .

5 Sélectionnez la règle dont vous voulez changer la priorité.

6 Cliquez sur **[Move up]** ou **[Move Down]** .

7 Cliquez sur **[Publish Changes]** .

Afficher les règles par type

Vous pouvez filtrer les règles pour afficher un sous-ensemble des règles. Toutes les règles sont affichées par défaut.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Firewall]** .

5 Cliquez sur **[Show]** et désélectionnez les options des règles à ne pas afficher.

Option	Description
All Rules	Affiche toutes les règles
Int Intf Rules	Affiche les règles qui s'appliquent à l'interface interne vShield.
Ext Intf Rules	Affiche les règles qui s'appliquent à l'interface externe vShield.
VPN Intf Rules	Affiche les règles qui s'appliquent à l'interface VPN.
Inbound Rules	Affiche les règles du trafic entrant dans le réseau virtuel.
Outbound Rules	Affiche les règles du trafic sortant du réseau virtuel.
Generated Rules	Affiche les règles générées par vShield Edge.

Supprimer une règle de pare-feu vShield Edge

Vous pouvez supprimer une règle de pare-feu personnalisée que vous avez ajoutée.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Firewall]** .

5 Sélectionnez la règle à supprimer.

6 Cliquez sur **[Delete Selected]** .

7 Cliquez sur **[Publish Changes]** .

Gestion des règles NAT

vShield Edge fournit un service NAT (network address translation) pour affecter une adresse publique à un ordinateur (ou un groupe d'ordinateurs) dans un réseau privé. Vous limitez ainsi le nombre d'adresses IP publiques qu'une organisation ou une entreprise doit utiliser pour des raisons économiques et de sécurité. Vous devez configurer les règles NAT pour fournir l'accès aux services hébergés sur des machines virtuelles à adresse privée.

La configuration du service NAT se sépare en règles SNAT et DNAT.

Ajouter une règle SNAT

Vous créez une règle SNAT pour convertir une adresse IP interne privée en adresse IP publique pour le trafic sortant.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes où un vShield Edge a été installé.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[NAT]** .

5 Sous SNAT, cliquez sur **[Add Rule]** .

La boîte de dialogue Add SNat Rule s'ouvre.

6 Tapez l'adresse **[Original (Internal) Source IP/Range]** . Pour entrer une plage d'adresses IP, séparez les adresses par une virgule.

7 Tapez l'adresse **[Translated (External) Source IP/Range]** . Pour entrer une plage d'adresses IP, séparez les adresses par un tiret.

8 Sélectionnez **[Log]** ou **[Do not log]** .

9 Cliquez sur **[OK]** pour enregistrer la règle.

10 Cliquez sur **[Publish Changes]** .

Ajouter une règle DNAT

Vous créez une règle DNAT pour mapper une adresse IP publique sur une adresse IP interne.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Mise en réseau]**

2 Sélectionnez un groupe de ports internes où vShield Edge a été installé.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[NAT]** .

5 Sous DNAT, cliquez sur **[Add Rule]** .

La boîte de dialogue Add DNat Rule s'affiche.

6 Tapez l'adresse **[Translated (Internal Destination) IP/Range]** .

7 Tapez le **[Port/Range]** interne.

8 Tapez le **[Original (External) Destination IP/Range]** .

9 Sélectionnez le **[Protocol]** .

10 Définissez les éléments suivants en fonction du protocole sélectionné.

Si le protocole est	Spécifiez
tcp ou udp	Port ou plage de ports
icmp	Type ICMP

11 Sélectionnez **[Log]** ou **[Do not log]** .

12 Cliquez sur **[OK]** pour enregistrer la règle.

Gestion du service DHCP

vShield Edge autorise le regroupement de pools d'adresses IP et l'attribution d'adresse IP statique bijective. La liaison d'adresse IP statique se base sur l'ID d'objet vCenter géré et l'ID d'interface du client demandeur.

Le service DHCP de vShield Edge respecte les règles suivantes :

- Écoute sur l'interface interne vShield Edge pour la découverte DHCP.
- Utilise l'adresse IP de l'interface interne dans vShield Edge comme adresse de passerelle par défaut pour tous les clients et les valeurs de diffusion et de masque de sous-réseau de l'interface interne pour le réseau conteneur.

Vous devez redémarrer le service DHCP sur les machines virtuelles clientes dans les cas suivants :

- Vous avez changé ou supprimé un pool DHCP, la passerelle par défaut ou les serveurs DNS.
- Vous avez changé l'adresse IP interne de vShield Edge.

Ajouter un pool IP DHCP

Le service DHCP nécessite un pool d'adresses IP qui sera affecté aux machines virtuelles protégées par un vShield Edge.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Mise en réseau]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[DHCP]** .

5 Sous DHCP Pools, cliquez sur **[Add Pool]** .

La fenêtre Add DHCP Pool s'affiche.

6 Tapez l'adresse **[Start IP]** .

7 Tapez l'adresse **[End IP]** .

8 Tapez le **[Domain Name]** .

9 Tapez le **[Primary Nameserver]** et le **[Secondary Nameserver]** qui font référence au service DNS. Vous devez saisir l'adresse IP d'un serveur DNS pour la résolution de nom d'hôte en adresse IP.

10 Dans l'adresse **[Default Gateway]** , tapez l'adresse IP interne du vShield Edge.

Si vous ne définissez pas l'adresse de **[passerelle par défaut]** , DHCP utilise l'adresse IP interne vShield Edge par défaut. Si vous redéfinissez l'adresse IP interne de vShield Edge, vous devez redémarrer les clients DHCP sur les machines virtuelles.

11 Pour **[Lease Time]** , indiquez si vous voulez louer l'adresse au client pour la durée par défaut (1 jour) ou spécifiez une valeur en secondes.

12 Cliquez sur **[OK]** .

Suivant

Vérifiez que le service DHCP a été activé. Pour plus d'informations, voir « Démarrer ou arrêter les services vShield Edge », page 47

Ajouter une liaison statique DHCP

Vous pouvez activer la liaison statique pour lier une adresse IP à l'adresse MAC d'une machine virtuelle.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[DHCP]** .

5 Sous DHCP Bindings, cliquez sur **[Add Binding]** .

6 Sélectionnez le **[VM Name]** que vous souhaitez lier.

7 Sélectionnez l' **[Interface]** pour laquelle vous voulez créer la liaison.

8 Tapez l' **[IP Address]** à laquelle vous voulez lier l'adresse MAC de la machine virtuelle sélectionnée.

9 Tapez le **[Domain Name]** .

10 Tapez le **[Primary Nameserver]** et le **[Secondary Nameserver]** qui font référence au service DNS. Vous devez saisir l'adresse IP d'un serveur DNS pour la résolution de nom d'hôte en adresse IP.

11 Tapez l'adresse de la **[Default Gateway]** .

12 Pour **[Lease Time]** , indiquez si vous voulez louer l'adresse au client pour la durée par défaut (1 jour) ou spécifiez une valeur en secondes.

13 Cliquez sur **[OK]** .

Suivant

Vérifiez que le service DHCP a été activé. Pour plus d'informations, voir « Démarrer ou arrêter les services vShield Edge », page 47

Gestion du service VPN

Les modules de vShield Edge prennent en charge l'établissement de réseau privé virtuel VPN IPSec d'un site à l'autre entre un vShield Edge et des sites distants.

vShield Edge prend en charge l'authentification de certificat, le mode de clé prépartagée, le trafic IP monodiffusion, mais aucun protocole de routage dynamique entre vShield Edge et les routeurs VPN distants. Derrière chaque routeur VPN distant, vous pouvez configurer plusieurs sous-réseaux pour connexion au réseau interne derrière un vShield Edge par des tunnels IPSec. Ces sous-réseaux et le réseau interne derrière un vShield Edge doivent avoir des plages d'adresses sans recouvrement.

Vous pouvez déployer un agent vShield Edge derrière un équipement NAT. Dans ce type de déploiement, l'équipement NAT traduit les adresses VPN d'un vShield Edge en adresses accessibles publiquement depuis l'Internet. Les routeurs VPN distants utilisent cette adresse publique pour accéder au vShield Edge.

Les routeurs VPN distants peuvent aussi se trouver derrière un équipement NAT. Vous devez fournir l'adresse native du VPN et l'ID de passerelle VPN pour configurer le tunnel. Des deux côtés, une traduction NAT statique bijective est indispensable pour l'adresse du VPN.

Vous pouvez disposer de 64 tunnels maximum sur 10 sites.

Configurer le service VPN sur un vShield Edge

Vous devez configurer une adresse IP externe sur le vShield Edge pour fournir le service VPN.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Mise en réseau]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[VPN]** .

5 Sous **[Global Configuration]** , cliquez sur **[Enable VPN]** .

La boîte de dialogue Add VPN Configuration s'affiche.

6 Tapez l'adresse IP de l'instance vShield Edge dans **[Local Service IP Address]** .

7 Tapez la clé prépartagée dans **[PSK for Sites with any Peer IP]** si des sites anonymes doivent se connecter au service VPN.

8 Tapez le nom de la connexion VPN dans **[VPN Gateway ID]** .

9 Sélectionnez **[Log]** pour consigner l'activité VPN.

10 Cliquez sur **[OK]** .

Suivant

Complétez le certificat d'authentification et envoyez le certificat signé.

Configurer un certificat d'authentification

Pour pouvoir utiliser l'authentification de certificat pour votre service VPN, vous pouvez générer une demande de signature de certificat, télécharger la demande, la faire signer et envoyer le certificat signé.

Générer une demande de signature de certificat (CSR)

1 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

2 Cliquez sur l'onglet **[vShield Edge]** .

3 Cliquez sur le lien **[VPN]** .

4 Dans l'option **[Actions]** , sous **[Global Configuration]** , sélectionnez **[Generate CSR]** .

5 Remplissez le formulaire de génération d'une demande de signature de certificat.

6 Cliquez sur **[Generate]** .

Le certificat de serveur Web de vShield Manager est remplacé par le nouveau certificat.

REMARQUE VMware recommande de redémarrer vShield Manager après la génération d'un certificat.

Télécharger une demande de signature de certificat générée

1 Dans l'option **[Actions]** sous **[Global Configuration]** , sélectionnez **[Download Generated CSR]** .

2 Cliquez sur **[Copy CSR Text to Clipboard]** pour copier le certificat vers le presse-papiers. Vous devez l'envoyer à une autorité de certification (CA) qui vous renverra le certificat signé.

Envoyer un certificat d'autorité de certification et un certificat signé

1 Dans l'option **[Actions]** sous **[Global Configuration]** , sélectionnez **[Upload Signed Certificate]** .

2 Selon le type de certificat que vous souhaitez charger, cliquez sur l'onglet approprié.

3 Dans **[Certificate file text]** , collez le texte du certificat.

4 Cliquez sur **[Upload.]**

Le certificat s'affiche dans la liste des certificats chargés.

5 Cliquez sur **[Save]** .

Ajouter un site homologue et un tunnel VPN

Une configuration VPN de bout en bout nécessite ou plusieurs sites homologues distants pour se connecter à vShield Edge via Internet.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[VPN]** .

5 Développez **[Peer Sites and Tunnels]** .

6 Cliquez sur **[Add Site]** .

7 Tapez un nom pour identifier le site dans **[Peer Site name]** .

8 Tapez le **[Peer Id]** pour identifier de manière unique le site homologue.

Pour les homologues utilisant l'authentification de certificat, cet ID doit être le nom commun dans le certificat de l'homologue. Pour les homologues PSK, cet ID peut être une chaîne. VMware recommande d'utiliser l'adresse IP publique du réseau VPN ou un nom de domaine qualifié complet (FQDN) pour le service VPN comme ID d'homologue.

9 Tapez l'adresse d'un site homologue dans **[Peer IP Address]** . Si vous ne définissez pas d'adresse, vShield Edge attend que le périphérique homologue demande une connexion.

10 Tapez l'adresse IP du sous-réseau homologue dans **[Peer subnets]** .

11 Tapez l'adresse de sous-réseau de vShield Edge dans **[Local subnets]** .

12 Tapez le seuil de l'unité de transmission maximale dans **[MTU]** . Si vous ne définissez pas la MTU, la MTU de l'interface externe vShield Edge est utilisée.

13 Sélectionnez **[Encryption algorithm]** .

14 Dans **[Authentication Method]** , sélectionnez l'un des éléments suivants :

Option	Description
PSK (Pre Shared Key)	Indique que la clé secrète partagée entre vShield Edge et le site homologue doit être utilisée pour l'authentification. La clé secrète peut être une chaîne d'une longueur maximale de 128 octets.
Certificate	Indique que le certificat défini au niveau global doit être utilisé pour l'authentification.

15 Dans **[Diffie-Hellman (DH) Group]** , sélectionnez le schéma de cryptographie qui permet au site homologue et à vShield Edge d'établir un secret partagé sur un canal de communication non protégé.

16 Indiquez si vous voulez activer ou désactiver le seuil **[Perfect Forward Secrecy (PFS)]** (secret de transmission parfait). Dans les négociations IPsec, Perfect Forward Secrecy (PFS) vérifie que chaque nouvelle clé cryptographique n'est pas associée à une clé précédente.

17 Cliquez sur **[OK]** .

vShield Edge crée un tunnel du sous-réseau local vers le sous-réseau homologue.

Suivant

Après avoir identifié un site homologue VPN, vous devez ajouter des règles de pare-feu pour indiquer comment le trafic doit transiter entre le sous-réseau local et le sous-réseau homologue.

Ajouter une route statique.

Vous pouvez définir une route statique que doivent suivre les paquets de données.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Static Routing]** .

5 Cliquez sur **[Add Route]** .

6 Tapez l'adresse IP **[Network]** .

7 Tapez l'adresse IP du **[Next Hop]** .

8 Pour **[Interface]** , sélectionnez **[Internal]** ou **[External.]**

9 Pour **[MTU]** , sélectionnez **[Use default value]** ou tapez la valeur de transmission maximale des paquets de données.

10 Cliquez sur **[Publish Changes]** .

Gérer le service d'équilibrage de charge

vShield Edge fournit un équilibrage de charge pour le trafic http. L'équilibrage de charge (jusqu'au niveau 7) permet l'extensibilité automatique des applications web.

Vous pouvez faire correspondre une adresse IP externe (ou publique) à un ensemble de serveurs internes pour l'équilibrage de charge. L'équilibrage de charge accepte les requêtes HTTP sur l'adresse IP externe et décide du serveur interne à utiliser. Le port 80 est le port d'écoute par défaut pour le service d'équilibrage de charge.

Configurer le service d'équilibrage de charge

Le service d'équilibrage de charge nécessite au moins deux serveurs pour distribuer le trafic HTTP. Vous pouvez identifier au moins deux machines virtuelles derrière un vShield Edge pour le service d'équilibrage de charge.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Load Balancer]** .

5 Cliquez sur **[Add Configuration]** .

6 Tapez les **[External IP Addresses]** .

7 Sélectionnez l'algorithme d'équilibrage de charge.

8 (Facultatif) Cochez la case Logging pour envoyer un événement syslog pour chaque requête à l'adresse IP externe.

9 Cliquez sur **[Add]** .

10 Tapez l'adresse IP du premier serveur Web.

11 Cliquez sur **[Add]** .

Vous pouvez ajouter des serveurs web supplémentaires de la même façon.

12 Cliquez sur **[Commit]** .

13 Si le service d'équilibrage de charge n'a pas été activé, activez-le.

Reportez-vous à la section « Démarrer ou arrêter les services vShield Edge », page 47.

Démarrer ou arrêter les services vShield Edge

Vous pouvez démarrer et arrêter les services VPN, DHCP et d'équilibrage de charge d'un vShield Edge depuis vSphere Client. Par défaut, tous les services sont arrêtés ou ont l'état Not Configured. Lorsque vous configurez un service, vShield Edge démarre le service.

Remarque Vous devriez configurer un service avant de le démarrer.

La stratégie de pare-feu par défaut bloque tout le trafic. Après avoir configuré un service VPN, DHCP ou d'équilibrage de charge, vous devez ajouter les règles de pare-feu correspondantes pour que le trafic transite et que le chemin de données puisse fonctionner pour ces services.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Status]** .

5 Sous Edge Services, sélectionnez un service et cliquez sur **[Start]** pour démarrer ce service.

Sélectionnez un service et cliquez sur **[Stop]** pour arrêter un service actif.

6 Cliquez sur **[Refresh Status]** pour actualiser l'état d'un service dans vShield Edge.

7 Si un service a été démarré mais qu'il ne répond pas ou si le service est désynchronisé par rapport à ce que montre vShield Manager, cliquez sur **[Force Sync]** pour envoyer une demande de synchronisation depuis vShield Manager à vShield Edge.

Redéployer vShield Edge

Si vShield Edge ne se trouve pas dans l'inventaire vCenter, vous devez redéployer the vShield Edge.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Networking]** .

2 Sélectionnez un groupe de ports internes protégés par un vShield Edge.

3 Cliquez sur l'onglet **[vShield Edge]** .

4 Cliquez sur le lien **[Status]** .

5 Cliquez sur **[Re-deploy]** .

Gestion de vShield App 9

vShield App est un pare-feu basé sur un hyperviseur qui protège les applications dans le centre de données virtuel contre les attaques provenant du réseau. Les organisations disposent d'une visibilité et d'un contrôle sur les communications réseau entre les machines virtuelles. Vous pouvez créer des stratégies de contrôle d'accès en fonction de constructions logiques, telles que des conteneurs VMware vCenter™ et des groupes de sécurité vShield et pas seulement des constructions physiques, telles que des adresses IP. En outre, l'adressage IP souple donne la possibilité d'utiliser la même adresse IP pour plusieurs zones client pour simplifier le provisionnement.

Vous devez installer vShield App sur tous les hôtes ESX d'un cluster pour que les opérations VMware vMotion puissent être exécutées et que les machines virtuelles restent protégées lors de la migration entre des hôtes ESX. Par défaut, un dispositif virtuel vShield App ne peut pas être déplacé à l'aide de vMotion.

La fonction Flow Monitoring affiche l'activité réseau entre les machines virtuelles au niveau du protocole d'application. Vous pouvez utiliser cette information pour auditer le trafic du réseau, définir et optimiser des stratégies de pare-feu et identifier les botnets (réseaux de machines zombies).

Ce chapitre aborde les rubriques suivantes :

- « Envoi des événements système vShield App à un serveur Syslog », page 49
- « Affichage de l'état système en cours d'une vShield App », page 50
- « Redémarrer une vShield App », page 50
- « Forcer la synchronisation d'une vShield App avec vShield Manager », page 50
- « Affichage des statistiques du trafic en fonction de l'interface vShield App », page 51
- « Configuration du mode Prévention de défaillance du pare-feu vShield App », page 51
- « Exclusion de machines virtuelles de la protection vShield App », page 51
- « Télécharger les journaux du support technique de vShield App », page 52

Envoi des événements système vShield App à un serveur Syslog

Vous pouvez envoyer les événements système vShield App à un serveur Syslog.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez un hôte dans l'arborescence des ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Dans la zone **[Service Virtual Machines]** , développez la SVM vShield App.

5 Dans la zone des serveurs Syslog, tapez l'adresse IP du serveur Syslog.

6 Dans le menu déroulant **[Log Level]** sélectionnez le niveau d'événement auquel et au-dessus duquel les événements vShield App doivent être envoyés au serveur syslog.

Si vous sélectionnez par exemple **[Emergency]** , seuls les événements de niveau urgence sont envoyés au serveur syslog. Si vous sélectionnez **[Critical]** , les événements de niveau critique, alerte et urgence sont envoyés au serveur syslog.

Vous pouvez envoyer des événements vShield App à trois instances syslog au maximum.

7 Cliquez sur **[Save]** pour enregistrer les nouveaux paramètres.

Affichage de l'état système en cours d'une vShield App

L'option **[System Status]** permet de voir et d'influencer le fonctionnement d'une vShield App. Les détails inclus sont notamment les statistiques système, l'état des interfaces, la version du logiciel et des variables d'environnement.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Sélectionnez un hôte dans l'arborescence des ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Dans la zone **[Service Virtual Machines]** , développez la SVM vShield App.

Le panneau Resource Utilization affiche les détails du système de la vShield App.

Redémarrer une vShield App

Vous pouvez redémarrer une vShield App pour dépannage d'un problème d'exploitation.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Sélectionnez un hôte dans l'arborescence des ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Dans la zone **[Service Virtual Machines]** , développez la SVM vShield App.

5 Cliquez sur **[Restart]** .

Forcer la synchronisation d'une vShield App avec vShield Manager

L'option **[Force Sync]** force une vShield App à se resynchroniser avec vShield Manager. Ceci peut être nécessaire après une mise à niveau de logiciel.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Sélectionnez un hôte dans l'arborescence des ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Dans la zone **[Service Virtual Machines]** , développez la SVM vShield App.

5 Cliquez sur **[Force Sync]** .

Affichage des statistiques du trafic en fonction de l'interface vShield App

Vous pouvez afficher les statistiques de trafic pour chaque interface vShield.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Sélectionnez un hôte dans l'arborescence des ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Dans la zone **[Service Virtual Machines]** , développez la SVM vShield App.

Le panneau Management Port Interface affiche les statistiques de trafic de la vShield App.

Configuration du mode Prévention de défaillance du pare-feu vShield App

Par défaut, le trafic est bloqué lorsque le dispositif vShield App est défaillant ou indisponible. Vous pouvez changer le mode Prévention de défaillance pour autoriser le trafic.

Procédure

1 Connectez-vous à vShield Manager.

2 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

3 Cliquez sur l'onglet **[App Global Configuration]** .

4 Dans **[App Fail Policy]** , cliquez sur **[Change fail policy to allow]** .

Exclusion de machines virtuelles de la protection vShield App

Vous pouvez exclure un groupe de machines virtuelles de la protection vShield App. Cette liste d'exclusion est appliquée à toutes les installations vShield App dans le vShield Manager spécifié. Si une machine virtuelle dispose de plusieurs vNIC, tous ces cartes virtuelles sont exclues de la protection.

vShield Manager et les machines virtuelles de service sont automatiquement exclues de la protection vShield App. Vous devez exclure le serveur vCenter et les machines virtuelles de service partenaires également pour autoriser le trafic.

Procédure

1 Connectez-vous à vShield Manager.

2 Cliquez sur **[Settings & Reports]** dans le panneau d'inventaire vShield Manager.

3 Cliquez sur l'onglet **[App Global Configuration]** .

4 Dans **[Virtual Machines Exclusion List]** , cliquez sur **[Add.]**

La boîte de dialogue Ajouter les machines virtuelles à exclure s'affiche.

5 Cliquez sur le champ à côté de Sélectionner et sur la machine virtuelle à exclure.

6 Cliquez sur **[Select.]**

La machine virtuelle sélectionnée est ajoutée à la liste.

7 Cliquez sur **[OK]** .

Télécharger les journaux du support technique de vShield App

Vous pouvez télécharger les journaux de support technique de chaque hôte sur lequel vous avez installé vShield App.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Sélectionnez un hôte dans l'arborescence des ressources.

3 Dans les machines virtuelles de service, cliquez sur **[Download Support logs]** .

4 Cliquez sur **[Log file generated; click here to download]** .

5 Ouvrez ou enregistrez le fichier journal.

vShield App Flow Monitoring 10

Flow Monitoring est un outil d'analyse de trafic fournissant une vue détaillée du trafic sur votre réseau virtuel et traversant une vShield App. La sortie de Flow Monitoring définit les machines qui échangent des données ainsi que les applications utilisées. Ces données incluent le nombre de sessions, de paquets et d'octets transmis par session. Les détails de session sont notamment les sources, destinations, sens des sessions, applications et ports utilisés. Les détails de session peuvent permettre de créer des règles d'autorisation ou d'interdiction de App Firewall.

Vous pouvez utiliser Flow Monitoring comme outil d'étude a posteriori pour détecter des services interdits et examiner les sessions sortantes.

Ce chapitre aborde les rubriques suivantes :

- « Description de l'affichage Flow Monitoring », page 53
- « Changement de la plage de dates dans les graphiques de Flow Monitoring », page 54
- « Afficher une application spécifique dans les graphiques Flow Monitoring », page 54
- « Afficher le rapport de Flow Monitoring », page 55
- « Supprimer tous les flux enregistrés », page 56

Description de l'affichage Flow Monitoring

L'onglet **[Flow Monitoring]** s'affiche tant que des statistiques sont renvoyées par un vShield App.

Flow Monitoring affiche les statistiques de trafic dans trois graphiques :

Sessions/hr	nombre total de sessions par heure
Server KBytes/hr	nombre de kilo-octets sortant par heure
Client/hr	nombre de kilo-octets entrant par heure

Flow Monitoring trie les statistiques par protocoles d'application utilisés dans les communications client-serveur, chaque couleur d'un graphique représentant un protocole d'application différent. Cette méthode de tracé de graphique permet de suivre vos ressources de serveur par application.

Les statistiques de trafic affichent toutes les sessions inspectées dans la plage temporelle spécifiée. Les sept derniers jours de données sont affichées par défaut.

Changement de la plage de dates dans les graphiques de Flow Monitoring

Vous pouvez changer la plage de dates des graphiques de Flow Monitoring pour une vue historiques des données de trafic.

Procédure

1 Dans vSphere Client, sélectionnez un centre de données, une machine virtuelle, un groupe de ports ou une carte réseau.

Option	Action
Sélectionner un centre de données ou une machine virtuelle	Accédez à **[Inventaire] > [Hôtes et clusters]**
Sélectionner un groupe de ports ou une carte réseau	Accédez à **[Inventaire] > [Networking]**

2 Cliquez sur l'onglet **[vShield]** .

3 Cliquez sur **[Flow Monitoring]** .

Les graphiques sont mis à jour pour afficher les dernières données des sept derniers jours. Ceci peut prendre quelques secondes.

4 En regard de **[Time Period]** , tapez une nouvelle date de début dans la zone de texte de gauche.

Cette date est la plus reculée dans le passé de début de la requête.

5 Dans la zone de texte de droite, tapez une nouvelle date de fin.

Cette date correspond à la dernière date d'arrêt de la requête.

6 Cliquez sur **[Update]** .

Afficher une application spécifique dans les graphiques Flow Monitoring

Vous pouvez sélectionner une application spécifique à afficher dans les graphiques en cliquant sur le menu déroulant **[Application]** .

Procédure

1 Dans vSphere Client, sélectionnez un centre de données, une machine virtuelle, un groupe de ports ou une carte réseau.

Option	Action
Sélectionner un centre de données ou une machine virtuelle	Accédez à **[Inventaire] > [Hôtes et clusters]**
Sélectionner un groupe de ports ou une carte réseau	Accédez à **[Inventaire] > [Networking]**

2 Cliquez sur l'onglet **[vShield]** .

3 Cliquez sur **[Flow Monitoring]** .

4 Dans le menu déroulant **[Application]** , sélectionnez l'application à afficher.

Les graphiques de Flow Monitoring sont actualisés pour afficher les données correspondant à l'application sélectionnée

Afficher le rapport de Flow Monitoring

Vous pouvez générer le rapport de surveillance de flux pour afficher les paquets autorisés, bloqués et usurpés enregistrés par vos instances de vShield App.

Procédure

1 Dans vSphere Client, sélectionnez un centre de données, une machine virtuelle, un groupe de ports ou une carte réseau.

Option	Action
Sélectionner un centre de données ou une machine virtuelle	Accédez à **[Inventory] > [Host and Clusters]**
Sélectionner un groupe de ports ou une carte réseau	Accédez à **[Inventory] > [Networking]**

2 Cliquez sur l'onglet **[vShield]** .

3 Cliquez sur **[Flow Monitoring]** .

Les graphiques se mettent à jour pour afficher les données les plus récentes des sept derniers jours. Ceci peut prendre quelques secondes.

4 Cliquez sur **[Show Report]** .

5 Détaillez le rapport.

6 S'il s'agit d'une machine virtuelle ou d'une carte réseau, cliquez sur **[Show Latest]** pour mettre à jour les statistiques du rapport

Affichage des données dans le rapport Flow Monitoring

Le rapport de Flow Monitoring présente les statistiques de trafic sous forme de tableau.

Le rapport permet le détail des statistiques de trafic selon la hiérarchie suivante :

1 Sélectionnez l'action du pare-feu : **[Allowed]** , **[Blocked]** ou **[Spoofed.]**

2 Sélectionnez un protocole L2 ou L3.

3 Si un protocole L2/L3 a été sélectionné, sélectionnez un protocole L2/L3 ou type de message.

4 Sélectionnez le sens du trafic : **[Incoming]** ou **[Outgoing]** .

5 Sélectionnez le type de port. **[Categorized]** (ports standard) ou **[Uncategorized]** (ports non standard).

6 Sélectionnez une application, un port ou un groupe de ports.

7 Sélectionnez un système d'exploitation.

8 Sélectionnez une adresse IP destination.

Pour un protocole TCP ou UDP, vous pouvez créer une règle App Firewall au niveau de l'adresse IP de destination.

Ajout d'une règle App Firewall depuis le rapport de Flow Monitoring

En détaillant les données de trafic, vous pouvez évaluer l'utilisation de vos ressources et envoyer les informations de session à App Firewall pour créer une nouvelle règle d'autorisation ou d'interdiction de niveau 3. La création de règles App Firewall à partir des données de Flow Monitoring est disponible seulement au niveau de centre de données pour les protocoles TCP et UDP.

Procédure

1 Connectez-vous à l'interface utilisateur vShield Manager..

2 Sélectionnez une ressource de centre de données du panneau d'inventaire .

3 Cliquez sur **[Flow Monitoring]** .

Les graphiques se mettent à jour pour afficher les données les plus récentes des sept derniers jours. Ceci peut prendre quelques secondes.

4 Cliquez sur **[Show Report]** .

5 Développez la liste Firewall action.

6 Développez la liste des protocoles de transport.

7 Développez la liste de sens du trafic.

8 Développez la liste Port type.

9 Développez la liste des applications ou des groupes de ports.

10 Développez la liste des adresse IP source ou de destination. Il s'agit de l'adresse IP d'une machine virtuelle dans votre réseau.

11 Cliquez sur **[Add Rule]** dans la colonne **[Firewall]** pour sélectionner une adresse IP de destination permettant de créer une règle App Firewall.

Une fenêtre contextuelle s'ouvre. Cliquez sur **[OK]** pour poursuivre.

La fenêtre Add s'ouvre.

REMARQUE L'option **[Add Rule]** est disponible uniquement pour les protocoles TCP et UDP.

12 Remplissez le formulaire pour configurer la règle de pare-feu. Pour plus d'informations, voir « Utilisation des règles de pare-feu d'application », page 64.

13 Cliquez sur OK.

Supprimer tous les flux enregistrés

Au niveau centre de données, vous pouvez supprimer les données pour toutes les sessions de trafic enregistrées dans le centre de données. Ceci efface les données des graphiques, du rapport et de la base de données. Généralement, vous effectuez cette opération lorsque vous transférez le déploiement vShield App de l'environnement de laboratoire vers l'environnement de production. Si vous devez conserver un historique des sessions de trafic, n'utilisez pas cette fonction.

Procédure

1 Sélectionnez une ressource de centre de données du panneau d'inventaire.

2 Cliquez sur l'onglet **[Flow Monitoring]** .

3 Cliquez sur **[Delete All Flows]** .

4 Cliquez sur **[Ok]** dans la fenêtre contextuelle pour confirmer la suppression.

AVERTISSEMENT Vous ne pouvez pas récupérer les données de trafic après un clic sur **[Delete All Flows]** .

Gestion du pare-feu vShield App 11

vShield App assure une protection de pare-feu par l'application de stratégies d'accès. L'onglet App Firewall représente la liste de contrôle d'accès du pare-feu vShield App.

Ce chapitre aborde les rubriques suivantes :

- « Utilisation de App Firewall », page 59
- « Utilisation des applications », page 61
- « Regroupement des objets », page 63
- « Utilisation des règles de pare-feu d'application », page 64
- « Utilisation de SpoofGuard », page 65

Utilisation de App Firewall

Le service App Firewall est un pare-feu centralisé hiérarchique pour les hôtes ESX. App Firewall permet de créer des règles d'autorisation ou d'interdiction d'accès depuis ou vers vos machines virtuelles. Chaque vShield App installée applique les règles de App Firewall.

Vous pouvez gérer les règles de App Firewall au niveau du centre de données, du cluster et du groupe de ports pour disposer d'un ensemble cohérent de règles sur plusieurs instances de vShield App sous ces conteneurs. Du fait que l'appartenance à ces conteneurs peut être modifiée dynamiquement, App Firewall maintient l'état des sessions existantes sans exiger de reconfiguration des règles de pare-feu. De cette façon, App Firewall dispose d'une empreinte continue efficace sur chaque hôte ESX sous les conteneurs administrés.

Espaces de noms dans un environnement mutualisé

Dans un mode mutualisé, vShield App permet d'affecter une adresse IP indépendante à des groupes de ports spécifiques.

Par défaut, tous les groupes de ports dans un centre de données partagent la même adresse IP. Vous pouvez affecter un espace de noms indépendant à un groupe de ports ; dans ce cas les règles de pare-feu au niveau du centre de données ne s'appliquent plus à ce groupe de ports. Vous pouvez utiliser la fonction d'espace de noms avec des groupes de sécurité pour distinguer les règles de pare-feu par client.

Pour affecter une adresse IP indépendant à un groupe de ports

1 Dans vSphere Client, accédez à **[Inventaire]** > **[Networking.]**

2 Sélectionnez un groupe de ports dans l'arborescence de ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur **[Namespace.]**

5 Cliquez sur **[Change to Independent namespace]** .

6 Cliquez sur **[Reload]** pour afficher les informations mises à jour.

À propos des applications

vShield App permet de créer des applications puis de définir des règles de pare-feu pour ces applications.

Tous les mappages personnalisés de paire application-port que vous avez définis dans un niveau précédent s'affichent comme applications par défaut.

Vous pouvez créer une application au niveau du centre de données ou du groupe de ports. Si vous créez une application pour un groupe de ports avec un espace de noms indépendant, la portée de l'application se limite à ce groupe de ports.

Création de groupes de sécurité

Pour créer des règles App Firewall, vous pouvez le faire en fonction du trafic vers ou depuis un conteneur spécifique intégrant toutes les ressources incluses dans ce conteneur. Vous pouvez par exemple créer une règle pour interdire tout trafic de l'intérieur d'un cluster visant une destination précise en dehors de ce cluster. Vous pouvez créer une règle pour interdire tout trafic entrant non étiqueté avec un ID de VLAN. Quand vous spécifiez un conteneur comme source ou destination, toutes les adresses IP de ce conteneur sont incluses dans la règle.

Un groupe de sécurité est une zone de confiance que vous créez et à laquelle vous attribuez des ressources pour la protéger avec App Firewall. Les groupes de sécurité sont des conteneurs, tout comme un vApp ou un cluster. Les groupes de sécurité vous permettent de créer un conteneur en attribuant arbitrairement des ressources, par exemple machines et adaptateurs réseau virtuels. Après la définition du groupe de sécurité, vous pouvez ajouter le groupe en tant que conteneur dans le champ source ou destination d'une règle App Firewall. Pour plus d'informations, voir « Regroupement des objets », page 63.

La portée du groupe de sécurité est limitée au niveau de la ressource où elle est créée. Si, par exemple, vous créez un groupe de sécurité au niveau du centre de données, le groupe de sécurité peut être ajouté comme source ou destination uniquement lorsque vous créez une règle de pare-feu au niveau du centre de données. Si vous créez une règle pour un groupe de ports dans ce centre de données, le groupe de sécurité n'est pas disponible.

À propos des règles définies par le système dans App Firewall

Par défaut, App Firewall applique un ensemble de règles qui autorise le trafic à passer par toutes les instances de vShield App. Ces règles figurent dans la section **[System Defined]** L3 et L2 de la table App Firewall. Les règles par défaut ne peuvent être ni supprimées ni ajoutées. Mais vous pouvez modifier l'élément **[Action]** de chaque règle de **[Allow]** à **[Deny]** .

À propos des règles de niveau 3 et de niveau 2

L'onglet **[App Firewall]** propose plusieurs ensembles de règles configurables : les règles de niveau 3 (L3) et les règles de niveau 2 (L2). Les niveaux font référence aux niveaux du modèle OSI (Open Systems Interconnection).

Par défaut, tout le trafic L3 et L2 est autorisé. Vous pouvez configurer des règles de couche 3 au niveau du centre de données, du groupe de ports et du cluster et des règles de couche 2 au niveau du centre de données et du groupe de ports.

Hiérarchie des règles App Firewall

Chaque vShield App applique les règles de App Firewall dans l'ordre de haut en bas. Une vShield App vérifie chaque session de trafic en fonction de la règle du haut dans la table App Firewall avant de passer aux règles suivantes de la table. La première règle de la table correspondant aux paramètres du trafic est appliquée.

Les règles sont appliquées dans la hiérarchie suivante :

1 **[High Precedence]**

2 **[Cluster]**

3 **[Network]**

4 **[Low Precedence]**

5 **[System Defined]**

App Firewall propose des configurations de priorité au niveau du conteneur et personnalisées :

- La priorité au niveau du conteneur désigne la possibilité de reconnaître le niveau de centre de données comme de priorité supérieure au niveau du cluster. Quand une règle est configurée au niveau du centre de données, elle est héritée par tous les clusters et les agents vShield qu'ils contiennent. Une règle au niveau du cluster n'est appliquée qu'à vShield App dans ce cluster.
- La priorité personnalisée désigne la possibilité d'affecter une priorité haute ou basse aux règles du niveau centre de données. Les règles de haute priorité fonctionnent comme indiqué dans la description de priorité au niveau du conteneur. Les règles de basse priorité incluent les règles par défaut ainsi que la configuration des règles de basse priorité de centre de données. Cette flexibilité permet de définir plusieurs niveaux de priorité appliquée.

  Au niveau du cluster, vous configurez les règles applicables à toutes les instances de vShield App dans le cluster. Du fait que les règles de haute priorité de centre de données sont au-dessus des règles de niveau cluster, assurez-vous que vos règles de niveau cluster n'entrent pas en conflit avec les règles de haute priorité du centre de données.

Planification de l'application de règles App Firewall

App Firewall permet de configurer des règles d'autorisation et d'interdiction en fonction de votre stratégie réseau.

Les exemples ci-dessous présentent deux stratégies courantes de pare-feu :

Autoriser tout le trafic par défaut	Vous conservez les règles par défaut qui autorisent tout et ajoutez des règles d'interdiction en fonction des données de surveillance de flux ou de configuration de règle manuelle de App Firewall. Dans ce scénario, si une session ne correspond à aucune des règles d'interdiction, vShield App autorise le passage du trafic.
Refuser tout le trafic par défaut	Vous pouvez remplacer l'état **[Action]** des règles par défaut en le faisant passer de **[Allow]** à **[Deny]** et ajouter des règles explicitement pour des systèmes et des applications donnés. Dans ce scénario, si une session ne correspond pas aux règles d'autorisation, vShield App coupe la session avant qu'elle atteigne sa destination. Si vous modifiez toutes les règles par défaut pour interdire tout trafic, vShield App coupe tout trafic entrant et sortant.

Utilisation des applications

Vous pouvez créer une application, puis définir des règles pour cette application.

Créer une application

Tous les mappages personnalisés de paire application-port que vous avez définis dans un niveau précédent s'affichent comme applications par défaut.

Procédure

1 Dans vSphere Client, passez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données du panneau d'inventaire.

3 Cliquez sur l'onglet **[Applications]** .

4 Cliquez sur **[Add]** .

La fenêtre Add Application s'ouvre.

5 Tapez un **[Name]** pour identifier l'application.

6 (Facultatif) Tapez la **[Description]** de l'application.

7 (Facultatif) Sélectionnez le **[Protocol]** auquel vous voulez ajouter un port non standard.

8 Tapez le ou les numéros de port dans **[Ports]** =.

9 Cliquez sur **[Save]** .

L'application personnalisée apparaît dans la table Applications.

Modifier une application

Vous pouvez modifier uniquement des applications personnalisées.

Procédure

1 Dans vSphere Client, passez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données du panneau d'inventaire.

3 Cliquez sur l'onglet **[Applications]** .

4 Sélectionnez une application personnalisée et cliquez sur **[Edit]**

La fenêtre Edit Application s'ouvre.

5 Effectuez les modifications nécessaires.

6 Cliquez sur **[OK]** .

Supprimer une application

Vous pouvez supprimer uniquement des applications personnalisées.

Procédure

1 Dans vSphere Client, passez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données du panneau d'inventaire.

3 Cliquez sur l'onglet **[Applications]** .

4 Sélectionnez une application personnalisée et cliquez sur **[Delete]**

La boîte de dialogue Delete Application s'affiche.

5 Cliquez sur **[Yes]** .

L'application est supprimée.

Regroupement des objets

La fonction de regroupement permet de créer des conteneurs personnalisés auxquels vous pouvez affecter des ressources, telles que des machines virtuelles et des adaptateurs réseau, pour la protection App Firewall. Après avoir défini un groupe, vous pouvez ajouter le groupe sous la forme d'une source ou d'une destination à une règle de pare-feu à des fins de protection.

Créer un groupe IP

Vous pouvez créer un groupe d'adresses IP constitué d'une plage d'adresse IP gb. Ensuite, vous pouvez ajouter ce groupe comme source ou destination dans une règle de pare-feu.

Procédure

1 Cliquez sur une ressource centre de données depuis vSphere Client.

2 Cliquez sur l'onglet **[vShield]** .

3 Cliquez sur l'onglet **[Grouping]** .

4 Cliquez sur **[Add]** et sélectionnez **[IP Addresses]** .

La fenêtre Ajouter des adresses IP s'affiche.

5 Tapez le nom du groupe d'adresses.

6 Tapez la description du groupe d'adresses.

7 Tapez les adresses IP à inclure dans le groupe.

8 Cliquez sur **[OK]** .

Créer un groupe de sécurité

Dans vSphere Client, vous pouvez ajouter un groupe de sécurité au niveau du centre de données ou du groupe de ports.

La portée du groupe de sécurité est limitée au niveau de la ressource où elle est créée. Si, par exemple, vous créez un groupe de sécurité au niveau du centre de données, le groupe de sécurité peut être ajouté comme source ou destination uniquement lorsque vous créez une règle de pare-feu au niveau du centre de données. Si vous créez une règle pour un groupe de ports dans ce centre de données, le groupe de sécurité n'est pas disponible.

Procédure

1 Cliquez sur une ressource centre de données depuis vSphere Client.

2 Cliquez sur l'onglet **[vShield]** .

3 Cliquez sur l'onglet **[Grouping]** .

4 Cliquez sur **[Add]** et sélectionnez **[Security Group]** .

La fenêtre Add Security Group s'ouvre avec le centre de données sélectionné affiché comme **[Scope]** .

5 Tapez le nom et la description du groupe de sécurité.

6 Cliquez sur **[Next]** .

7 Cliquez dans le champ à côté du bouton Add et sélectionnez la ressource à inclure dans le groupe de sécurité.

8 Cliquez sur **[Add]** . La ressource sélectionnée apparaît dans la liste sous le bouton Add. Vous pouvez ajouter plusieurs ressources au groupe de sécurité.

Lorsque vous ajoutez une ressource à un groupe de sécurité, toutes les ressources associées sont ajoutées automatiquement. Par exemple, lorsque vous sélectionnez une machine virtuelle, la vNIC associée est ajoutée automatiquement au groupe de sécurité.

9 Cliquez sur **[Finish]**

Utilisation desrègles de pare-feu d'application

Vous pouvez ajouter des règles de pare-feu L3 et L2 à priorité basse ou élevée.

Ajout d'une règle de pare-feu d'application

Vous pouvez ajouter une règle de pare-feu d'application à divers niveaux de conteneur.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Hôtes et clusters]** et sélectionnez un centre de données ou accédez à **[Inventaire] > [Networking]** et sélectionnez un groupe de ports.

2 Cliquez sur l'onglet **[vShield App]** .

3 Cliquez sur **[App Firewall]** .

4 Dans la zone Haute priorité, Réseau ou Basse priorité, cliquez sur **[Add Rule]** .

La fenêtre Add Rule s'ouvre.

Remarque Après avoir créé une règle dans l'une de ces zones, vous devez cliquez sur le bouton **Add** au-dessus de la colonne Source pour ajouter d'autres règles.

5 Remplissez le formulaire pour configurer la règle de pare-feu.

Option	Description
Source	Conteneur ou adresse IP source de la communication.
Limite de la source	Direction par rapport à la source d'origine de la communication.
Destination	Conteneur ou adresse IP visée par la communication.
Limite de la destination	Direction par rapport à la destination visée par la communication.
Protocole	Protocole de la règle.
Journalisation	Indique si tous les sessions qui correspondent à la règle sont journalisées. L'activation de la journalisation peut affecter les performances.
Activé	Indique si la règle que vous créez doit être activée.
Remarques	Commentaires sur la règle.

6 Cliquez sur **[OK]** .

7 Sélectionnez la nouvelle règle et cliquez sur le bouton **[Move Up]** ou **[Move Down]** pour monter ou descendre la règle dans la priorité.

8 Cliquez sur **[Publish Changes]** pour envoyer la nouvelle règle à toutes les instances vShield App.

Supprimer une règle de pare-feu d'application

Vous pouvez supprimer toute règle de App Firewall que vous avez créée. Vous ne pouvez pas supprimer les règles de la section System Defined de la table.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez un centre de données ou un groupe de ports dans l'arborescences de ressources, selon le niveau auquel vous voulez supprimer une règle.

3 Cliquez sur l'onglet **[vShield App]** .

4 Cliquez sur **[App Firewall]** .

5 Cliquez sur une règle dans la table appropriée.

6 Cliquez sur **[Delete Selected]** .

Vous pouvez cliquer sur **[Delete All]** pour supprimer toutes les règles de pare-feu.

Revenir à une configuration précédente du pare-feu d'application

vShield Manager enregistre les paramètres du App Firewall chaque fois que vous publiez une nouvelle règle. Lorsque vous cliquez sur **[Publier changements]** , vShield Manager enregistre la configuration précédente avec un horodateur avant d'ajouter une nouvelle règle. Ces configurations sont disponibles dans la liste déroulante **[Historique]** .

Procédure

1 Dans vSphere Client, allez dans **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez un centre de données ou une ressource de clusters depuis le panneau d'inventaire.

3 Cliquez sur l'onglet **[App Firewall]** .

4 Cliquez sur **[Historique] > [Charger]** .

La boîte de dialogue Historique configuration pare-feu affiche les configurations précédentes dans l'ordre des horodateurs. La configuration la plus récente figure en haut de la liste.

5 Sélectionnez la configuration à laquelle vous souhaitez revenir.

6 Cliquez sur **[OK]** .

7 Dans la boîte de dialogue Charger configuration, cliquez sur **[OK]** .

8 Cliquez sur **[Publier changements]** .

La configuration sélectionnée est chargée.

Utilisation de SpoofGuard

Après synchronisation avec vCenter Server, vShield Manager recueille les adresses IP de toutes les machines virtuelles clients vCenter auprès de VMware Tools sur chaque machine virtuelle. Jusqu'à vShield 4.1, vShield faisait confiance à l'adresse IP fournie par VMware Tools sur une machine virtuelle. Mais si une machine virtuelle a été compromise, l'adresse IP peut être usurpée et des transmissions malicieuses peuvent passer à travers les stratégies de pare-feu.

SpoofGuard permet d'autoriser les adresses IP signalées par VMware Tools, et de les modifier si nécessaire pour éviter l'usurpation. SpoofGuard fait confiance essentiellement aux adresses MAC des machines virtuelles recueillies dans les fichiers VMX et le vSphere SDK. Du fait qu'il est séparé des règles App Firewall, vous pouvez utiliser SpoofGuard pour bloquer du trafic considéré comme usurpé.

Quand il est activé, vous pouvez utiliser SpoofGuard pour surveiller et gérer les adresses IP signalées par vos machines virtuelles dans un des modes suivants.

Automatically Trust IP Assignments On Their First Use Ce mode permet de faire passer tout le trafic de vos machines virtuelles pendant la construction d'une table d'affectation d'adresses MAC aux adresses IP. Vous pouvez consulter cette table quand vous le souhaitez pour apporter des modifications d'adresse IP.

Manually Inspect and Approve All IP Assignments Before Use Ce mode bloque tout le trafic jusqu'à approbation de chaque affectation d'adresse MAC à une adresse IP.

REMARQUE SpoofGuard autorise toutes les requêtes DHCP quel que soit le mode activé. Mais en mode d'inspection manuelle, le trafic ne passe pas tant que l'adresse IP attribuée par DHCP n'a pas été approuvée.

Options de l'écran SpoofGuard

L'interface SpoofGuard contient les options suivantes.

Tableau 11-1. Options de l'écran SpoofGuard

Option	Description
Active IP assignments	Liste de toutes les adresses IP valides.
Inactive IP Assignments	Liste des adresses IP ne correspondant pas aux adresses IP publiées.
Active Since Last Published	Liste des adresses IP validées depuis la dernière mise à jour de la stratégie
Unpublished IP assignment changes	Liste de machines virtuelles pour lesquelles vous avez modifié l'affectation d'adresse IP sans l'avoir publiée pour l'instant
IP assignments that require my review and approval	Modifications d'adresse IP nécessitant une approbation avant d'autoriser le trafic depuis ou vers ces machines virtuelles
Duplicate IP assignments	Adresses IP en double d'une adresse IP affectée existante dans le centre de données sélectionné

Activer SpoofGuard

Une fois activé, vous pouvez utiliser SpoofGuard pour gérer les affectations d'adresses IP de l'ensemble de l'inventaire vCenter .

IMPORTANT Vous devez mettre à niveau toutes les instances de vShield App en vShield App 1.0.0 Update 1 ou ultérieur avant de pouvoir activer SpoofGuard.

Procédure

1 Dans l'interface utilisateur vShield Manager, accédez à la vue **[Settings and Reports]** .

2 Cliquez sur l'onglet **[SpoofGuard]** .

3 Cliquez sur **[Edit]** à droite de l'en-tête Global Status.

4 Pour **[IP Assignment Tracking]** , cliquez sur **[Enable]** .

5 Pour **[Operation Mode]** , sélectionnez un des modes suivants :

Option	Description
Automatically Trust IP Assignments on Their First Use	Sélectionnez cette option pour faire confiance à toutes les affectations d'adresse IP lors de leur enregistrement initial sur vShield Manager.
Manually Inspect and Approve All IP Assignments Before Use	Sélectionnez cette option pour exiger une approbation manuelle de toutes les adresses IP. Tout le trafic provenant des adresses IP non approuvées ou y aboutissant est bloqué.

6 Cliquez sur **[OK]** .

Approbation d'adresses IP

Si vous demandez à SpoofGuard d'exiger une approbation manuelle de toutes les affectations d'adresse IP, vous devez approuver les affectations d'adresse pour permettre le passage du trafic de ces machines virtuelles.

Procédure

1 Dans vSphere Client, accédez à la vue **[Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données dans l'arborescence de ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur l'onglet **[SpoofGuard]** .

5 Cliquez sur le lien **[Require Approval]** ou **[Duplicate IP assignments]** .

6 Utilisez l'une des méthodes suivantes :

- Cochez la première case dans la colonne de cases à cocher de droite pour sélectionner toutes les affectations affichées.
- Cochez la case correspondant à chaque affectation que vous souhaitez approuver.

7 Cliquez sur **[Approve Selected]** .

8 Cliquez sur **[Publish Now]** .

Modifier une adresse IP

Vous pouvez modifier l'adresse IP affectée à une adresse MAC pour corriger cette adresse IP.

Remarque SpoofGuard accepte une adresse IP unique provenant de plus d'une machine virtuelle. Mais vous ne pouvez attribuer une adresse IP qu'une seule fois. Une adresse IP approuvée doit être unique sur le système vShield. Les adresses IP approuvées en double ne sont pas autorisées.

Procédure

1 Dans vSphere Client, accédez à la vue **[Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données dans l'arborescence de ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur l'onglet **[SpoofGuard]** .

5 Cliquez sur un des liens d'option.

6 Dans la colonne Approved IP, cliquez sur **[Edit]** .

7 Tapez une adresse IP dans la fenêtre contextuelle **[Approved IP Address]** .

8 Cliquez sur **[Apply]** .

9 Cliquez sur **[Publish Now]** .

Supprimer une adresse IP

Vous pouvez supprimer une affectation d'une adresse MAC à une adresse IP de la table SpoofGuard pour nettoyer la table d'une machine virtuelle qui n'est plus active. Toute instance supprimée peut réapparaître dans la table SpoofGuard en fonction du trafic affiché et de l'état activé en cours de SpoofGuard.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Hôtes et clusters]**

2 Sélectionnez une ressource de centre de données dans l'arborescence de ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur l'onglet **[SpoofGuard]** .

5 Cliquez sur un des liens d'option.

6 Dans la colonne Approved IP, cliquez sur **[Delete]** .

7 Cliquez sur **[Publish Now]** .

Événement et alarmes vShield Endpoint 12

vShield Endpoint transfère le traitement des agents antivirus et contre les logiciels malveillants vers un dispositif virtuel sécurisé et dédié, fourni par des partenaires VMware. Étant donné que le dispositif virtuel sécurisé (à la différence d'une machine virtuelle cliente) n'est pas déconnecté, il peut mettre à jour en permanence les signatures antivirus, assurant ainsi une protection ininterrompue des machines virtuelles sur l'hôte. Par ailleurs, les nouvelles machines virtuelles (ou les machines virtuelles existantes qui ont été déconnectées) sont protégées immédiatement contre la plupart des signatures antivirus actuelles lorsqu'elles sont connectées.

L'état d'intégrité de vShield Endpoint est transmis par des alarmes qui s'affichent en rouge sur la console vCenter Server. De plus, il est possible d'obtenir des informations d'état en consultant les journaux d'événements.

IMPORTANT Votre vCenter Server doit être configuré correctement pour la sécurité de vShield Endpoint :

- Tous les systèmes d'exploitation hébergés ne sont pas pris en charge par vShield Endpoint. Les machines virtuelles avec des systèmes d'exploitation non pris en charge ne sont pas protégées par la solution de sécurité. Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultez la section Installation de vShield Endpoint dans le *vShield Quick Start Guide*.
- Tous les hôtes d'un pool de ressources contenant des machines virtuelles protégées doivent être préparés pour vShield Endpoint afin que les machines virtuelles continuent à être protégées, étant donné qu'elles sont migrées avec vMotion à partir d'un hôte ESX sur un autre dans le pool de ressources.

Ce chapitre aborde les rubriques suivantes :

- « Afficher l'état de vShield Endpoint », page 69
- « Alarmes vShield Endpoint », page 70
- « Événements de vShield Endpoint », page 70
- « Messages d'audit de vShield Endpoint », page 71

Afficher l'état de vShield Endpoint

La surveillance d'une instance de vShield Endpoint implique la vérification de l'état signalé par les composants vShield Endpoint : la machine virtuelle de sécurité (SVM), le module vShield Endpoint résidant sur l'hôte ESX et l'agent léger résident sur la machine virtuelle protégée.

Procédure

1 Dans vSphere Client, accédez à **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez une ressource de centre de données, de cluster ou d'hôte ESX dans l'arborescence de ressources.

3 Cliquez sur l'onglet **[vShield]** .

4 Cliquez sur **[Endpoint]** .

La page de l'intégrité et des alarmes vShield Endpoint affiche l'intégrité des objets sous le centre de données, le cluster ou l'hôte ESX que vous avez sélectionné, ainsi que les alarmes actives.

Alarmes vShield Endpoint

Les alarmes signalent à l'administrateur de vCenter Server des événements vShield Endpoint exigeant son attention. Les alarmes sont annulées automatiquement si l'état d'alarme n'existe plus.

Les alarmes de vCenter Server peuvent être affichées sans plug-in vSphere. Voir le *Guide d'administration vCenter Server* pour les événements et alarmes.

Lors de l'enregistrement en tant qu'extension de vCenter Server, vShield Manager définit les règles permettant de créer et de supprimer des alarmes, en fonction des événements provenant des trois composants de vShield Endpoint : SVM, module vShield Endpoint et agent léger. Les règles peuvent être personnalisées. Pour savoir comment créer des règles personnalisées pour les alarmes, voir la documentation de vCenter Server. Dans certains cas, les alarmes peuvent avoir des causes multiples. Les tableaux ci-dessous donnent la liste des causes possibles avec des actions correspondantes pouvant être entreprises pour y remédier.

Alarmes d'hôte

Les alarmes d'hôte sont générées par des événements concernant l'état de bon fonctionnement du module vShield Endpoint.

Tableau 12-1. Erreurs (repérées en rouge)

Cause possible	Action
Le module vShield Endpoint a été installé sur l'hôte, mais ne signale plus d'état à vShield Manager.	1 Assurez-vous que vShield Endpoint fonctionne en vous connectant à l'hôte et en tapant la commande `/etc/init.d/vShield-Endpoint-Mux start` 2 Assurez-vous que le réseau est configuré correctement de sorte que vShield Endpoint puisse se connecter à vShield Manager. 3 Redémarrez vShield Manager.

Alarmes SVM

Les alarmes SVM sont générées par des événements qui affectent l'intégrité des SVM.

Tableau 12-2. Alarmes SVM rouges

Problème	Action
Il existe une discordance de version de protocole avec le module vShield Endpoint	Vérifiez que le module vShield Endpoint et la SVM utilisent des protocoles mutuellement compatibles.
vShield Endpoint n'a pas pu établir une connexion à la SVM	Vérifiez que la SVM est sous tension et que le réseau est configuré correctement.
La SVM ne communique pas son état, même si les clients sont connectés.	Erreur interne. Contactez le technicien de maintenance VMware.

Événements de vShield Endpoint

Les événements s'utilisent pour la journalisation et l'audit de conditions internes au système de sécurité basé sur vShield Endpoint.

Les événements peuvent être affichés sans plug-in vSphere personnalisé. Voir le *Guide d'administration vCenter Server* pour les événements et alarmes.

Les événements sont la base des alarmes générées. Lors de l'enregistrement en tant qu'extension de vCenter Server, vShield Manager définit les règles permettant de créer et de supprimer des alarmes.

Les arguments communs à tous les événements sont l'horodatage des événements et `event_id` vShield Manager.

Le tableau suivant répertorie les événements vShield Endpoint signalés par la SVM et vShield Manager (VSM).

Tableau 12-3. Événements de vShield Endpoint

Description	Gravité	Arguments VC
Solution vShield Endpoint *SolutionName* activée. Version sous-jacente *versionNumber* du protocole VFile.	info	horodatage
Module ESX activé.	info	horodatage
Module ESX désinstallé.	info	horodatage
vShield Manager a perdu la connexion au module ESX.	info	horodatage
La solution vShield Endpoint *SolutionName* a été contactée par une version non compatible du module ESX.	erreur	horodatage, version de la solution, version du module ESX
Une connexion entre le module ESX et *SolutionName* a échoué.	erreur	horodatage, version du module ESX, version de la solution
vShield Endpoint n'est pas parvenu à se connecter à la SVM.	erreur	horodatage
vShield Endpoint a perdu la connexion à la SVM.	erreur	horodatage

Messages d'audit de vShield Endpoint

Les messages d'audit incluent les erreurs fatales et autres messages d'audit importants, ils sont journalisés dans `vmware.log`.

Les conditions suivantes sont journalisées sous forme de message d'AUDIT :

- Réussite de l'initialisation de l'agent léger (et numéro de version).
- Échec de l'initialisation de l'agent léger.
- Établissement de la première communication avec la SVM.
- Échec d'établissement de la communication avec la SVM (au premier échec de ce genre).

Les messages générés dans le journal ou les sous-chaînes correspondantes près du début de chaque message de journal : `vf-AUDIT`, `vf-ERROR`, `vf-WARN`, `vf-INFO`, `vf-DEBUG`.

Gestion de vShield Data Security 13

vShield Data Security offre une visibilité dans les données sensibles stockées dans les environnements virtualisés et de nuage de votre organisation. Selon les violations signalées par vShield Data Security, vous pouvez garantir que les données sensibles sont protégées de manière adéquate et évaluer la conformité aux réglementations mondiales.

Pour commencer à utiliser vShield Data Security, vous : créez une règle qui définit les réglementations qui s'appliquent à la sécurité des données dans votre organisation et spécifie les zones de l'environnement et les fichiers à analyser. Une réglementation est constituée de lames de contenu qui identifient le contenu sensible à détecter. vShield prend en charge les réglementations PCI, PHI et PII uniquement.

Lorsque vous démarrez une analyse de la sécurité des données, vShield analyse les données sur les machines virtuelles de votre inventaire vSphere et signale le nombre de violations détectées et les fichiers qui ont violé la règle.

Vous pouvez exécuter toutes les tâches de sécurité en utilisant les API REST. Pour plus d'informations, consultez le Guide de programmation de l'API vShield.

Ce chapitre aborde les rubriques suivantes :

- « Rôles d'utilisateur vShield Data Security », page 74
- « Définition d'une stratégie de sécurité des données », page 74
- « Modification d'une stratégie de sécurité des données », page 76
- « Exécution d'une analyse de la sécurité des données », page 77
- « Affichage et téléchargement des rapports », page 77
- « Création d'expressions ordinaires », page 78
- « Réglementations disponibles », page 79
- « Lames d'analyse de contenu disponibles », page 96
- « Formats de fichier pris en charge », page 117

Rôles d'utilisateur vShield Data Security

Le rôle d'un utilisateur détermine les actions que l'utilisateur peut exécuter.

Rôle	Actions autorisées
Security Administrator	Créer et publier des stratégies et afficher des rapports de violation. Ne peut pas démarrer ni arrêter une analyse de la sécurité des données.
vShield Administrator	Démarrer et arrêter les analyses de la sécurité des données.
Auditor	Afficher les stratégies définies et les rapports de violation.

Définition d'une stratégie de sécurité des données

Pour pouvoir détecter les données sensibles dans votre environnement, vous devez créer une stratégie de sécurité des données. Vous devez être administrateur de sécurité pour pouvoir créer des stratégies.

Pour définir une stratégie, vous devez définir :

1 Réglementations

Une réglementation est une loi de protection des données personnelles pour protéger les informations PCI (Payment Card Industry), PHI (Protected Health Information) et PII (Personally Identifiable Information). Vous pouvez sélectionner les réglementations que doit respecter votre entreprise. Lorsque vous exécutez une analyse, vShield Data Security identifie les données qui violent les réglementations dans la stratégie et qui sont sensibles pour votre entreprise.

2 Zones participantes

Par défaut, l'ensemble de l'infrastructure vSphere est analysée par vShield Data Security. Pour analyser un sous-ensemble de l'inventaire, vous pouvez exclure ou inclure des groupes de sécurité. Si une ressource (cluster, centre de données ou hôte) fait partie à la fois d'un groupe de sécurité exclu et inclus, la liste d'exclusion prévaut et la ressource n'est pas analysée.

3 Des filtres de fichiers

Vous pouvez créer des filtres pour limiter les données analysées et exclure de l'analyse les types de fichiers qui ne contiennent vraisemblablement pas des données sensibles.

Sélectionner des réglementations

Lorsque vous sélectionnez des réglementations que doivent respecter les données de l'entreprise, vShield peut identifier les fichiers qui contiennent des informations qui violent ces réglementations.

Prérequis

Le rôle Administrateur de la sécurité doit vous avoir été affecté.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Sélectionnez un centre de données.

Remarque Même si vous sélectionnez un centre de données, la stratégie que vous définissez s'applique à l'ensemble de l'inventaire vSphere.

3 Cliquez sur l'onglet **[vShield App]** et sur **[Data Security]** .

4 Cliquez sur l'onglet **[Policy]** et développez **[Regulations and standards to detect]** .

5 Cliquez sur **[Edit]** et sur **[All]** pour afficher toutes les réglementations disponibles.

6 Sélectionnez les réglementations dont vous voulez vérifier la conformité.

Remarque Pour plus d'informations sur les réglementations disponibles, voir « Réglementations disponibles », page 79.

7 Cliquez sur **[Suivant]** .

8 Certaines réglementations nécessitent des informations supplémentaires pour vShield Data Security pour identifier les données sensibles. Si vous avez sélectionné une réglementation qui surveille les numéros d'assurances des groupes, les numéros de sécurité sociale de patients, les numéros des dossiers médicaux, les numéros des bénéficiaires des régimes de santé, les numéros de comptes bancaires, les comptes personnalisés ou les numéros de matricule des étudiants, définissez un modèle d'expression régulière pour identifier ces données.

Remarque Vérifiez l'exactitude de l'expression régulière. La définition d'expressions régulières incorrectes peut ralentir la découverte. Pour plus d'informations sur les expressions régulières, voir « Création d'expressions ordinaires », page 78.

9 Cliquez sur **[Finish]**

10 Si vous mettez à jour une stratégie existante, cliquez sur **[Publish Changes]** pour l'appliquer.

Spécifier les zones participant à l'analyse de politique

Par défaut, l'ensemble de l'infrastructure vSphere est analysée par vShield Data Security. Pour analyser un sous-ensemble de l'inventaire, vous pouvez exclure ou inclure des groupes de sécurité. Si une ressource (cluster, centre de données ou machine virtuelle) fait partie d'un groupe de sécurité exclu et inclus, la liste d'exclusion prévaut et la ressource n'est pas analysée.

Les dispositifs spéciaux vShield (tels que vShield Endpoint et Shield App, ainsi que les dispositifs partenaires qui exploitent vShield Endpoint, ne sont pas analysés par vShield Data Security

Prérequis

Le rôle Administrateur de la sécurité doit vous avoir été affecté.

Procédure

1 Dans l'onglet Policy du panneau Data Security, développez **[Participating Areas]** .

2 Pour inclure un groupe de sécurité dans l'analyse de sécurité des données, cliquez **[Change]** à côté de **[Scan the following infrastructure]** .

   a Dans la boîte de dialogue Security Groups, tapez le nom du groupe de sécurité à inclure dans l'analyse.

   b Cliquez sur **[Add]** .

   c Cliquez sur **[Save]** .

3 Pour exclure un groupe de sécurité de l'analyse de la sécurité des données, cliquez sur **[Change]** à côté de **[Except for the following areas]** .

   a Dans la boîte de dialogue Exclure des groupes de sécurité, tapez le nom du groupe de sécurité à exclure de l'analyse.

   b Cliquez sur **[Add]** .

   c Cliquez sur **[Save]** .

4 Si vous mettez à jour une stratégie existante, cliquez sur **[Publish Changes]** pour l'appliquer.

Spécifier des filtres de fichiers

Vous pouvez limiter les fichiers à surveiller en fonction de la taille, de la date de la dernière modification ou des extensions de fichier.

Prérequis

Le rôle Administrateur de la sécurité doit vous avoir été affecté.

Procédure

1 Dans l'onglet **[Policy]** du panneau de la sécurité des données, développez **[Files to scan]** .

2 Cliquez sur **[Edit]** .

3 Vous pouvez surveiller tous les fichiers sur les machines virtuelles de l'inventaire ou sélectionner les restrictions à appliquer.

Option	Description
Monitor all files on the guest virtual machines	vShield Data Security analyse tous les fichiers.
Monitor only the files that match the following conditions	Sélectionnez les options suivantes selon le cas. ■ **[Size]** indique que vShield Data Security ne doit analyser que les fichiers dont la taille est inférieure à la taille définie. ■ **[Last Modified Date]** indique que vShield Data Security doit analyser uniquement les fichiers modifiés entre les dates définies. ■ **[Types:]** Sélectionnez **[Only files with the following extensions]** pour entrer les types de fichiers à analyser. Sélectionnez **[All files, except those with extensions]** pour entrer les types de fichiers à exclure de l'analyse.

Pour plus d'informations sur les formats de fichier que peut détecter vShield Data Security, voir « Formats de fichier pris en charge », page 117.

4 Cliquez sur **[Save.]**

5 Si vous mettez à jour une stratégie existante, cliquez sur **[Publish Changes]** pour l'appliquer.

Modification d'une stratégie de sécurité des données

Après avoir défini une règle de sécurité de données, vous la modifiez en changeant les réglementations sélectionnées, les zones participant à l'analyse ou les filtres de fichier. Pour pouvoir appliquer la stratégie modifiée, vous devez la publier.

Prérequis

Vérifiez que vous avez affecté du rôle Administrateur de sécurité.

Procédure

1 Dans vSphere Client, sélectionnez **[Inventaire]** > **[Hôtes et clusters]** .

2 Sélectionnez un centre de données.

REMARQUE Même si vous sélectionnez un centre de données, la stratégie modifiée s'applique à l'ensemble de l'inventaire vSphere.

3 Cliquez sur l'onglet **[vShield App]** et sur **[Data Security]** .

4 Cliquez sur l'onglet **[Policy]** et développez les sections à modifier.

5 Effectuez les modifications nécessaires.

6 Cliquez sur **[Save]** .

7 Si vous mettez à jour une stratégie existante, cliquez sur **[Publish Changes]** pour l'appliquer.

REMARQUE Si vous publiez une stratégie pendant une analyse, l'analyse redémarre. Cette nouvelle analyse permet de vérifier que toutes les machines virtuelles respectent la stratégie modifiée.

Exécution d'une analyse de la sécurité des données

L'exécution d'une analyse de la sécurité des données identifie les données de l'environnement virtuel qui violent votre stratégie.

Prérequis

Vous devez être administrateur vShield pour pouvoir démarrer, suspendre ou arrêter une analyse de la sécurité des données.

Procédure

1 Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .

2 Cliquez sur l'onglet **[vShield App]** et sur **[Data Security]** .

3 Cliquez sur **[Start]** .

REMARQUE Si une machine virtuelle est hors tension, elle n'est pas analysée tant qu'elle n'est pas sous tension.

Si une analyse est en cours, les options disponibles sont **[Pause]** et **[Stop]** .

Toutes les machines virtuelles dans le centre de données sont analysées une seule fois au cours d'une analyse. Si vous modifiez la stratégie et la publiez pendant une analyse, l'analyse redémarre. Cette nouvelle analyse permet de vérifier que toutes les machines virtuelles respectent la stratégie modifiée. Une nouvelle analyse est déclenchée par la publication d'une stratégie modifiée et non par les mises à jour de données sur les machines virtuelles.

Si vous transférez une machine virtuelle vers un cluster ou un pool de ressources exclu pendant une analyse de la sécurité des données, les fichiers de la machine virtuelle ne sont pas analysés. Si vous transférez une machine virtuelle via vMotion vers un autre hôte, l'analyse se poursuit sur le second hôte (les fichiers analysés lorsque la machine virtuelle était sur l'hôte précédent ne sont pas analysés de nouveau).

Lorsque le moteur Data Security démarre l'analyse d'une machine virtuelle, il enregistre l'heure de début de l'analyse. Lorsque l'analyse prend fin, il enregistre la fin de l'analyse. Vous pouvez afficher les heures de début et de fin d'un cluster, d'un hôte ou d'une machine virtuelle en sélectionnant l'onglet **[Tasks and Events]** .

vShield Data Security régule le nombre de machines virtuelles analysées sur un seul hôte à la fois pour réduire l'impact sur les performances. VMware recommande de suspendre l'analyse pendant les heures de travail normales pour éviter d'affecter les performances.

Affichage et téléchargement des rapports

Lorsque vous démarrez une analyse de sécurité, vShield affiche les heures de début et de fin de l'analyse, le nombre de machines virtuelles analysées et le nombre de violations détectées.

Prérequis

Vérifiez que vous avez été affecté du rôle d'administrateur de sécurité ou d'auditeur.

Procédure

1 Dans vSphere Client, sélectionnez **[Inventaire] > [Hôtes et clusters]** .

2 Sélectionnez le centre de données, le cluster, le pool de ressources ou la machine virtuelle pour lesquels vous voulez afficher des rapports.

3 Cliquez sur **[Data Security]** .

4 Cliquez sur l'onglet **[Reports]** dans le panneau de la sécurité des données.

Tableau 13-1. Informations affichées dans l'onglet Rapports

Section	Informations affichées
État d'analyse en cours	État de l'analyse en cours.
Statistiques d'analyse	Le graphique à secteurs indique le nombre de machines virtuelles analysées, en cours d'analyse et à analyser.
Informations de violation	Il s'agit des principales réglementations qui ont été violées et des machines virtuelles sur lesquelles ces violations ont été détectées.
Historique d'analyse	Indique les heures de début et de fin de chaque analyse, le nombre de machines virtuelles analysées et le nombre de violations détectées. Vous pouvez cliquer sur **[Download Complete Report]** dans la colonne **[Action]** pour télécharger le rapport complet d'une analyse.

Création d'expressions ordinaires

Une expression ordinaire est un modèle qui décrit une certaine séquence de caractères textuels, encore appelée chaîne de caractères. Vous utilisez des expressions ordinaires pour rechercher, ou trouver des correspondances avec des chaînes spécifiques ou des catégories de chaînes dans un corps de texte.

L'utilisation d'une expression ordinaire s'apparente à une recherche générique, mais les expressions ordinaires sont bien plus puissantes. Les expressions ordinaires peuvent être très simples, ou très complexes. Un exemple d'expression ordinaire simple est *cat.*

Elle trouve la première occurrence de la séquence de lettres « cat » dans tout le corps de texte auquel s'applique la recherche. Si vous voulez vous assurer qu'elle ne trouve que le mot *cat*, et pas d'autres chaînes telles que *cats* ou *hepcat*, vous pouvez utiliser cette expression légèrement plus complexe : *\bcat\b*.

Cette expression inclut des caractères spéciaux qui permettent de s'assurer qu'il n'y a occurrence qu'en cas de rupture de mot des deux côtés de la séquence *cat*. À titre d'exemple supplémentaire, pour effectuer une recherche quasi-équivalente à la chaîne typique de recherche générique *c+t*, vous pouvez utiliser cette expression ordinaire : *\bc\w+t\b*.

Cela signifie trouver une limite de mot (\b) suivie d'un *c*, suivi d'un ou plusieurs caractères autre qu'un espace ou un caractère de ponctuation (\w+), suivis d'un *t*, suivi d'une limite de mot (\b). Cette expression trouve *cot*, *cat*, *croat*, mais pas *crate.*

Les expressions peuvent devenir très complexes. L'expression suivante trouve une adresse électronique valide.

\b[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b

Pour plus d'informations sur la création d'expressions ordinaires, voir http://userguide.icu-project.org/strings/regexp.

Réglementations disponibles

Les descriptions de chacune des réglementations disponibles dans vShield Data Security sont fournies ci-dessous.

Arizona SB-1338

La loi d'état de protection des données d'Arizona SB-1338 vise à protéger les informations personnellement identifiables. La loi Arizona SB-1338 a été adoptée le 26 avril 2006 et est entrée en vigueur le 31 décembre 2006. La loi s'applique à toute personne physique ou morale qui mène des activités en Arizona et détient ou octroie sous licence des données informatisées non chiffrées qui comprennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros de routage ABA

Un numéro de transit de routage (RTN) ou un numéro ABA est un code bancaire à neuf chiffres, utilisé aux États-Unis, qui apparaît sur des éléments tels que les chèques et qui identifie l'institution financière sur laquelle ils sont émis. Ce code est également utilisé par la chambre de compensation automatisée pour traiter les dépôts directs et les autres transferts automatisés. Le nom de ce système provient de l'association des banquiers américains (American Bankers Association), qui l'a conçu en 1910.

Il existe environ 24 000 numéros actifs de routage et de transit actuellement en circulation. Chaque institution financière en possède un : il s'agit d'un numéro à neuf chiffres imprimés avec la police MICR (reconnaissance de caractères magnétiques) au bas des chèques qui identifie spécifiquement l'institution financière à laquelle il est associé et qui est régi par le Conseil d'administration des numéros de routage sous l'égide de l'ABA.

Les principaux objectifs du numéro de routage sont les suivants :

- Identifier la banque qui est chargée de payer ou d'accorder un crédit ou qui est habilitée à recevoir un paiement ou un crédit pour une opération financière.
- Fournir une référence à un point de présentation désigné de la banque auquel l'opération peut être délivrée ou présentée.

Pour plus d'informations, voir « Lame d'analyse de contenu de numéro de routage ABA », page 96.

Numéros de compte bancaire australien

Un numéro de compte bancaire australien, ainsi qu'un BSB (numéro de succursale bancaire de l'État) identifie le compte bancaire d'un individu ou d'une organisation.

Numéros ABN (numéro d'identification d'entreprise australienne) et ACN (numéro de société australienne)

Les numéros ABN (numéro d'identification d'entreprise australienne) et ACN (numéro de société australien) identifient de façon unique les entreprises dans le pays.

Le numéro ABN est un numéro unique d'identification à 11 chiffres que les entreprises utilisent lorsqu'elles traitent avec d'autres entreprises. Les neuf derniers chiffres du numéro ABN d'une société représentent le plus souvent le numéro ACN de la société. Le numéro ABN indique qu'une personne, un groupe ou une société est enregistré auprès de l'ABR (Registre des entreprises australiennes).

Un numéro de société australienne (généralement abrégé par ACN) est un numéro unique à 9 chiffres émis par la Commission australienne des valeurs mobilières et des investissements (ASIC) et attribué comme identificateur à chaque société enregistrée, en vertu de la loi de 2001 relative aux entreprises du Commonwealth. Le numéro se présente généralement sous la forme de trois groupes de trois chiffres.

Les sociétés doivent indiquer leur ACN sur :

- le sceau social (s'il en existe un)
- chaque document public émis, signé ou publié par, ou au nom de, la société
- chaque effet bancable négociable, émis, signé ou publié par, ou au nom de, la société
- tous les documents qui doivent être déposés auprès de l'ASIC

Cette réglementation utilise les lames d'analyse de contenu intitulées ABN (numéro d'entreprise australien) ou ACN (numéro de société australien). Pour plus d'informations, voir.

Numéros de carte Medicare australienne

Tous les citoyens et résidents permanents en Australie et leur famille ont droit à une carte Medicare (carte d'assurance maladie), à l'exception des résidents de l'île Norfolk. La carte indique le nom d'une personne ainsi que celui des membres de sa famille qu'elle choisit d'ajouter, qui sont également des résidents permanents et correspondent à la définition de Medicare d'une personne dépendante (cinq noms au maximum). Il est nécessaire de fournir un Numéro Medicare pour obtenir une remise Medicare ou obtenir l'accès au système hospitalier public pour y recevoir des soins gratuitement en qualité de patient public.

Medicare est administré par Medicare Australia (connu sous le nom de Health Insurance Commission (Commission d'assurance santé) jusqu'à la fin de l'année 2005), à qui incombe également la responsabilité de fournir les cartes et les numéros Medicare. Quasiment toute personne admissible possède une carte : en juin 2002, 20,4 millions de détenteurs de carte Medicare ont été dénombrés, et la population australienne comptait moins de 20 millions d'habitants à ce moment-là (les détenteurs de carte comprennent les Australiens à l'étranger qui possèdent toujours une carte).

La carte Medicare est utilisée uniquement pour les soins médicaux et ne peut pas être utilisée pour un suivi dans une base de données. Elle contient un nom et un numéro, et aucune photographie visible (à l'exception de la version « Smartcard » tasmanienne qui renferme une image électronique du détenteur de la carte sur une puce intégrée).

L'objectif principal de la carte Medicare est de prouver l'admissibilité à Medicare lors de la recherche de soins assurés par un médecin ou un hôpital et financés par Medicare. Du point de vue légal, il n'est pas nécessaire de présenter la carte et un numéro Medicare suffit. En pratique, la plupart des prestataires Medicare disposeront de politiques exigeant la présentation de la carte pour prévenir la fraude.

Numéros de dossiers fiscaux australiens

Un numéro de dossier fiscal (TFN) est un numéro qui est attribué à une personne par le Commissaire aux impôts et est utilisé pour vérifier l'identité du client et établir son niveau de revenu.

Cette politique utilise la lame d'analyse de contenu intitulé Numéro de dossier fiscal australien. Voir la description des lames d'analyse de contenu pour comprendre quel contenu sera détecté.

California AB-1298

La loi d'état de protection des données de California AB-1298 vise à protéger les informations personnellement identifiables. La loi California AB-1298 a été adoptée le 14 octobre 2007 et est entrée en vigueur le 1er janvier 2008. La loi s'applique à toute personne, entreprise ou agence d'État qui mène des activités en Californie et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

Cette loi est une modification de la loi California SB-1386 destinée à inclure des renseignements médicaux et de santé dans la définition des informations personnelles.

La réglementation recherche au moins une correspondance avec des informations personnellement identifiables, telles que définies par les lames d'analyse de contenu suivantes :

- Dates d'admission et d'autorisation de sortie
- Numéros de carte de crédit
- Données de piste de carte de crédit
- Numéros d'assurance de groupe
- Numéros des bénéficiaires du régime de soins médicaux
- Dictionnaires des soins de santé
- Historique médical
- Numéros d'identification des patients
- Numéros de permis de conduire américains
- Identificateurs des prestataires nationaux américains
- Numéros de sécurité sociale américains

California SB-1386

La loi d'état de protection des données de California SB-1386 vise à protéger les informations personnellement identifiables. La loi California SB-1386 a été adoptée le 25 septembre 2002 et est entrée en vigueur le 1er juillet 2003. La loi s'applique à toute personne, entreprise ou agence d'État qui mène des activités en Californie et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

Cette loi a été modifiée de façon à inclure des renseignements médicaux et de santé ; elle est maintenant désignée sous l'appellation de California AB-1298, qui est délivrée en tant que réglementation étendue dans le SDK. Si California AB-1298 est activé, il n'est pas nécessaire d'utiliser aussi cette réglementation car les mêmes informations sont détectées dans le cadre de loi AB-1298.

La réglementation recherche au moins une correspondance avec les informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit

- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros d'assurance sociale canadienne

Un Numéro d'assurance sociale (NAS) est un numéro émis au Canada pour gérer divers programmes gouvernementaux. Le NAS a été créé en 1964 pour servir de numéro de compte client dans l'administration du Régime de retraite du Canada et les divers programmes d'assurance-emploi du Canada. En 1967, Revenue Canada (désormais l'Agence du revenu du Canada) a commencé à utiliser le NAS à des fins de déclaration fiscale.

Numéros de permis de conduire canadien

Au Canada, les permis de conduire sont délivrés par le gouvernement de la province dans laquelle le conducteur réside. Ainsi, les réglementations spécifiques relatives aux permis de conduire varient d'une province à l'autre, bien qu'ils soient plutôt similaires dans l'ensemble. Toutes les provinces prévoient des dispositions autorisant les non-résidents à utiliser les permis délivrés par d'autres provinces et les permis de conduire internationaux.

La réglementation recherche au moins une correspondance avec une des lames d'analyse de contenu suivantes :

- Permis de conduire de la Province d'Alberta
- Permis de conduire de la Province de la Colombie Britannique
- Permis de conduire de la Province du Manitoba
- Permis de conduire de la Province du Nouveau Brunswick
- Permis de conduire de la Province de Terre-Neuve-et-Labrador
- Permis de conduire de la Province de la Nouvelle-Écosse

  Règles de modèle du numéro de permis : 5 lettres suivies de 9 chiffres
- Permis de conduire de la Province de l'Ontario
- Permis de conduire de la Province de l'île du Prince-Edouard
- Permis de conduire de la Province de Québec
- Permis de conduire de la province du Saskatchewan

Colorado HB-1119

La loi d'état de protection des données de Colorado HB-1119 vise à protéger les informations personnellement identifiables. La loi Colorado HB-1119 a été adoptée le 24 avril 2006 et est entrée en vigueur le 1er septembre 2006. La loi s'applique à toute personne physique ou entité commerciale qui mène des activités dans le Colorado et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

La réglementation recherche au moins une correspondance avec les informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Connecticut SB-650

La loi d'état de protection des données de Connecticut SB-650 vise à protéger les informations personnellement identifiables. La loi Connecticut SB-650 a été adoptée le 8 juin 2005 et est entrée en vigueur le 1er janvier 2006. La loi s'applique à toute personne, entreprise ou agence qui mène des activités dans le Connecticut et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

La réglementation recherche au moins une correspondance avec des informations personnellement identifiables, telles que définies par les lames d'analyse de contenu suivantes :

- Dates d'admission et d'autorisation de sortie
- Certificats de naissance et de décès
- Numéros de carte de crédit
- Données de piste de carte de crédit
- Numéros d'assurance de groupe
- Numéros des bénéficiaires du régime de soins médicaux
- Dictionnaires des soins de santé
- Historique médical
- Numéros d'identification des patients
- Numéros de permis de conduire américains
- Identificateurs des prestataires nationaux américains
- Numéros de sécurité sociale américains

Numéros de carte de crédit

Numéros de compte personnalisé

Si vous avez des numéros de compte d'organisation qui doivent être protégés, personnalisez alors la lame de contenu affectée à la réglementation Numéros de compte personnalisé avec le modèle du numéro via une expression ordinaire.

Numéros de carte de paiement de l'UE

La politique recherche des numéros de carte de paiement émis par les principaux organismes émetteurs de cartes de paiement de l'Union Européenne tels que Maestro, Visa et Laser.

FERPA (Loi sur les Droits de la famille et protection des données dans l'éducation)

La FERPA protège les renseignements personnels des étudiants dans les établissements d'enseignement qui reçoivent des fonds du Ministère de l'Éducation américain. Elle exige que l'établissement d'enseignement ait une autorisation écrite d'un parent ou d'un étudiant pour communiquer des renseignements appartenant au dossier scolaire ou universitaire d'un étudiant.

Dans certaines circonstances, les informations telles que le nom, l'adresse, le numéro de téléphone, les distinctions et récompenses, et les dates de présence peuvent être communiquées ou publiées sans autorisation. Les informations permettant d'identifier un individu faisant l'objet d'un classement ou de mesures disciplinaires nécessitent une autorisation.

La politique doit concorder avec les deux lames suivantes d'analyse de contenu pour qu'un document déclenche une violation :

- Numéros d'identification de l'étudiant
- Dossiers de l'étudiant

Florida HB-481

La loi d'état de protection des données Florida HB-481 vise à protéger les informations personnellement identifiables. La loi Florida HB-481 a été adoptée le 14 juin 2005 et est entrée en vigueur le 1er juillet 2005. La loi s'applique à toute personne physique, entreprise, association, coentreprise, partenariat, consortium, personne morale, et tout autre groupe ou combinaison qui mène des activités en Floride et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros IBAN français

Un numéro IBAN (Numéro de compte bancaire international) français est une norme internationale permettant d'identifier les comptes bancaires français au-delà des frontières nationales et a été adopté à l'origine par le Comité européen pour les normes bancaires. Le registre officiel IBAN dans le cadre de l'ISO 13616:2003 est publié par la SWIFT (Société des télécommunications mondiales financières interbancaires – Society for Worldwide Interbank Financial Telecommunication).

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro IBAN français ».

Politique concernant les numéros d'identification nationaux français

La politique identifie les documents et les transmissions qui contiennent des numéros d'identification nationaux, appelés également numéros INSEE ou numéros de sécurité sociale, qui sont délivrés à chaque personne à sa naissance par l'INSEE (Institut National de la Statistique et des Études Économiques) en France.

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro d'identification national français ».

Politique Georgia SB-230

La loi d'état de protection des données de Georgia SB-230 vise à protéger les informations personnellement identifiables. La loi Georgia SB-230 a été adoptée le 5 mai 2005 et est entrée en vigueur le 5 mai 2005. La loi s'applique à toute personne physique ou morale qui, en échange de frais monétaires ou de redevances, exerce totalement ou partiellement des activités de collecte, d'assemblage, d'évaluation, de compilation, de diffusion, de transmission, de transfert, ou de communication d'informations concernant des individus dans l'objectif principal de fournir des informations personnellement identifiables à des tiers extérieurs, ou à une agence ou sous-division locale ou d'état qui tient à jour des données qui incluent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Politique concernant les numéros BIC allemands

Un Code d'identification des banques (BIC) identifie de manière unique une banque particulière et est utilisé en France et dans le monde entier pour les échanges de fonds et de messages entre banques. La politique identifie les documents et les transmissions qui contiennent des codes BIC, également connus sous le nom de codes SWIFT, émis par la SWIFT (Société des télécommunications mondiales financières interbancaires – Society for Worldwide Interbank Financial Telecommunication).

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro BIC allemand ».

Politique concernant les numéros de permis de conduire en Allemagne

Un Numéro de permis de conduire en Allemagne est le numéro d'identification sur un permis de conduire allemand et il identifie le propriétaire dudit numéro pour les besoins de conduite et des infractions à la conduite.

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro de permis de conduire en Allemagne ».

Politique concernant les numéros IBAN allemands

Un numéro IBAN (Numéro de compte bancaire international) est une norme internationale permettant d'identifier les comptes bancaires au-delà des frontières nationales et a été adopté à l'origine par le Comité européen pour les normes bancaires. Le registre officiel IBAN dans le cadre de l'ISO 13616:2003 est publié par la SWIFT (Société des télécommunications mondiales financières interbancaires – Society for Worldwide Interbank Financial Telecommunication).

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro IBAN allemand ».

Politique concernant les numéros d'identification nationaux allemands

La politique identifie des documents et des transmissions qui contiennent des numéros d'identification personnels, ou Personalausweis, délivrés à chaque personne en Allemagne.

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro d'identification national allemand ».

Politique concernant les numéros de TVA allemands

basée sur l'entreprise ou la personne morale pour la perception de la Taxe sur la valeur ajoutée (ou la taxe sur les biens et services).

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro de TVA allemand ».

Politique concernant la loi Hawaii SB-2290

La loi d'état de protection des données de Hawaii SB-2290 vise à protéger les informations personnellement identifiables.

La loi Hawaii SB-2290 a été adoptée le 25 mai 2006 et est entrée en vigueur le 1er janvier 2007. La loi s'applique à toute entreprise individuelle, tout partenariat, toute personne morale, association, ou tout autre groupe, structuré, et constitué ou non pour être à but lucratif, y compris les institutions financières qu'elles soient structurées, agréées, ou détiennent une licence ou un certificat d'autorisation en vertu des lois hawaïennes ou de tout autre état, des États-Unis ou de tout autre pays, ou de la société mère ou de la filiale de toute institution financière de ce type, et de toute entité dont l'activité concerne la destruction de données, ou toute agence gouvernementale qui collecte des informations personnellement identifiables à des fins gouvernementales spécifiques

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Politique HIPAA (Healthcare Insurance Portability and Accountability Act)

La loi HIPPA a été promulguée par le Congrès des États-Unis d'Amérique. La loi HIPAA inclut une règle de confidentialité réglementant l'utilisation et la communication des renseignements médicaux protégés (PHI), une règle de sécurité définissant les mécanismes de sécurité requis pour les renseignements médicaux protégés électroniques (ePHI), et une règle d'application qui définit les procédures pour les recherches de violation et les dommages-intérêts pour les violations confirmées.

Les renseignements médicaux protégés sont définis comme étant des informations de santé individuellement identifiables, qui sont transmises ou conservées sous toute forme ou sur tout support (électronique, oral ou papier) par une entité couverte ou ses associés, non comprises certaines données relatives à l'éducation et à l'emploi. Par « individuellement identifiables », on entend que l'identité du sujet est ou peut être aisément déterminée par l'enquêteur ou associée à l'information.

Cette politique est élaborée pour détecter les renseignements médicaux protégés électroniques, qui contiennent un numéro médical personnel en plus d'une terminologie de santé. Certains faux négatifs peuvent se produire car des combinaisons d'informations personnellement identifiables, telles que le nom et l'adresse, ne sont pas considérées comme des renseignements médicaux protégés électroniques dans cette politique. Les recherches internes indiquent que la plupart des communications médicales contiendront un numéro médical personnel en plus d'une terminologie de santé.

Politique concernant la loi Idaho SB-1374

La loi d'état de protection des données d'Idaho SB-1374 vise à protéger les informations personnellement identifiables. La loi Idaho SB-1374 a été adoptée le 30 mars 2006 et est entrée en vigueur le 1er juillet 2006. La loi s'applique à toute agence, personne physique ou entité commerciale qui mène des activités dans l'Idaho et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables sur un résident de l'Idaho.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Illinois SB-1633

La loi d'état de protection des données d'Illinois SB-1633 vise à protéger les informations personnellement identifiables. La loi Illinois SB-1633 a été adoptée le 16 juin 2005 et est entrée en vigueur le 27 juin 2006.

La loi s'applique à toute structure de collecte de données, qui inclut, mais sans limitation aux agences gouvernementales, universités publiques et privées, sociétés cotées et non cotées, institutions financières, opérateurs de détail, et à toute autre entité qui, à quelque fin que ce soit, assure la gestion, la collecte, la diffusion, ou autrement s'occupe d'informations personnellement identifiables non publiques, qui détient ou octroie sous licence des informations personnellement identifiables concernant un résident de l'Illinois.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Politique concernant la loi Indiana HB-1101

La loi d'état de protection des données d'Indiana HB-1101 vise à protéger les informations personnellement identifiables. La loi Indiana HB-1101 a été adoptée le 26 avril 2005 et est entrée en vigueur le 1er juillet 2006. La loi s'applique à toute personne physique, morale, fiducie d'entreprise, ayants cause, trust, partenariat, association, organisation ou société à but non lucratif, ou à toute autre entité légale qui détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Politique concernant les numéros de permis de conduire italien

Un Numéro de permis de conduire italien est le numéro d'identification sur un permis de conduire italien et identifie le propriétaire dudit numéro pour les besoins de conduite et des infractions de conduite.

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro de permis de conduire italien ».

Politique concernant les numéros IBAN italiens.

Un numéro IBAN (Numéro de compte bancaire international) est une norme internationale permettant d'identifier les comptes bancaires au-delà des frontières nationales et a été adopté à l'origine par le Comité européen pour les normes bancaires. Le registre officiel IBAN ISO 13616:2003 est publié par la SWIFT (Société des télécommunications mondiales financières interbancaires – Society for Worldwide Interbank Financial Telecommunication).

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro IBAN italien ».

Politique concernant les numéros d'identification nationaux italiens

La politique identifie des documents et des transmissions qui contiennent des numéros d'identification personnels, ou Codice Fiscale, délivrés à chaque personne en Italie.

La politique recherche une correspondance avec la lame d'analyse de contenu « Numéro d'identification national italien ».

Politique concernant la loi Kansas SB-196

La loi d'état de protection des données de Kansas SB-196 vise à protéger les informations personnellement identifiables. La loi Kansas SB-196 a été adoptée le 19 avril 2006 et est entrée en vigueur le 1er janvier 2007. La loi s'applique à toute personne physique, partenariat, personne morale, trust, ayants cause, coopérative, association, gouvernement, ou sous-division ou agence gouvernementale ou à toute autre entité qui mène des activités au Kansas et détient ou octroie sous licence des données informatisées non chiffrées comprenant des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Règle Louisiana SB-205

La loi d'état de protection des données Louisiana SB-205 vise à protéger les informations personnellement identifiables. Approuvée le 12 juillet 2005 et entrée en vigueur le 1er janvier 2006, elle s'applique à tout individu, société, partenariat, entreprise individuelle, société de capitaux, société en participation ou toute autre entité légale qui fait des affaires en Louisiane et détient ou certifie des données informatisées non cryptées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit

- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Règle : Maine LD-1671

La loi d'état de protection des données Maine LD-1671 vise à protéger les informations personnellement identifiables. Approuvée le 10 juin 2005 et entrée en vigueur le 31 janvier 2006,

elle s'applique à tout individu, partenariat, société, société à responsabilité limitée, société de fiducie, patrimoine, coopérative, association ou autre entité, y compris les agences de gouvernement d'état, l'UMS (University of Maine System), le MCCS (Maine Community College System), la MMA (Maine Maritime Academy), et les écoles et universités privées, ou toute information tout ou en partie dans la collecte, l'assemblage, l'évaluation, la compilation, le reporting, la transmission, le transfert ou la communication d'informations concernant les personnes avec pour objectif principal de fournir personnellement des informations identifiables à des tiers non affiliés qui maintiennent des données informatisées contenant des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Massachusetts CMR-201

La réglementation d'état de protection des données Massachusetts CMR-201 vise à protéger les informations personnellement identifiables. Approuvée le 19 septembre 2008 et entrée en vigueur le 1er mai 2009, elle s'applique à toutes les entreprises et autres entités légales qui détiennent, certifient, collectent, stockent ou conservent des informations personnelles relatives à un résident du Commonwealth du Massachusetts.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéros de routage ABA
- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéros de comptes bancaires américains
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Minnesota HF-2121

La loi d'état de protection des données Minnesota HF-2121 vise à protéger les informations personnellement identifiables. Approuvée le 2 juin 2005 et entrée en vigueur le 1er janvier 2006, elle s'applique à toute personne ou société qui fait des affaires dans le Minnesota et détient ou certifie des données qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit

- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Montana HB-732

La loi d'état de protection des données Montana HB-732 vise à protéger les informations personnellement identifiables. Approuvée le 28 avril 2005 et entrée en vigueur le 1er mars 2006, elle s'applique à toute personne ou société qui fait des affaires dans le Montana et détient ou certifie des données informatisées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros de permis de conduire des Pays-Bas

Le numéro de permis de conduire des Pays-Bas est un numéro d'identification sur un permis de conduire néerlandais. Il identifie le propriétaire dudit numéro pour la conduite et toute infraction au code de la route.

La règle cherche une correspondance dans le commutateur de contenu du numéro de permis de conduire des Pays-Bas.

Nevada SB-347

La loi d'état de protection des données Nevada SB-347 vise à protéger les informations personnellement identifiables. Approuvée le 17 juin 2005 et entrée en vigueur le 1er octobre 2005, elle s'applique à toute agence de gouvernement, institution d'éducation supérieure, société, institution financière ou ventes au détail, ou tout autre type d'entité ou association commerciale qui détient ou

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

New Hampshire HB-1660

La loi d'état de protection des données New Hampshire HB-1660 vise à protéger les informations personnellement identifiables. Approuvée le 2 juin 2006 et entrée en vigueur le 1er janvier 2007, elle s'applique à tout individu, société, société de fiducie, partenaire, association avec ou sans personnalité morale, société à responsabilité limitée et autre forme d'entité, ou toute agence, autorité, conseil d'administration, cour, service, division, commission, institution, bureau, ou autre entité gouvernementale, ou toute section politique de l'état faisant des affaires dans le New Hampshire et qui détient ou certifie des données informatisées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit

- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

New Jersey A-4001

La loi d'état de protection des données New Jersey A-4001 vise à protéger les informations personnellement identifiables.

Approuvée le 22 septembre 2005 et entrée en vigueur le 1er janvier 2006, elle s'applique au New Jersey, et dans tout pays, municipalité, district, autorité publique, agence publique et toute autre section politique ou du corps public du New Jersey, toute entreprise individuelle, partenariat, société, association ou autre entité, cependant organisée ou non pour réaliser des bénéfices, y compris une institution financière organisée, agréée ou détenant une licence ou un certificat d'autorisation sous la loi du New Jersey, de tout autre état, des États-Unis, ou de tout autre pays, ou le parent ou la filiale d'une institution financière, qui fait des affaires dans le New Jersey compilant ou conservant des enregistrements informatiques qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

New York AB-4254

La loi d'état de protection des données New York AB-4254 vise à protéger les informations personnellement identifiables. Approuvée le 10 août 2005 et entrée en vigueur le 8 décembre 2005, elle s'applique à toute personne ou société qui fait des affaires dans l'état de New York et détient ou certifie des données informatisées non cryptées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros de service des recettes fiscales de Nouvelle-Zélande

La règle identifie les documents et les transmissions qui contiennent les numéros de Service des recettes fiscales de Nouvelle-Zélande (IRD) émis par le Service des recettes fiscales à chaque contribuable et à chaque organisation. Le numéro doit être fourni par un individu aux Recettes fiscales, employeurs, banques ou autres institutions financières, fournisseurs de régime KiwiSaver, StudyLink et agents fiscaux.

La règle cherche une correspondance dans la lame d'analyse de contenu du numéro du service des recettes fiscales de Nouvelle-Zélande.

Numéros du ministère de la santé de Nouvelle-Zélande

La règle identifie les documents et les transmissions qui contiennent les numéros de l'Indice des Praticiens de la Santé (IPH) ou de l'Indice National de la Santé (INSA) de Nouvelle-Zélande.

Le ministère de la Santé de Nouvelle-Zélande, ou Manatu Hauora en Maori, est l'agent et conseiller principal du gouvernement néo-zélandais en matière de santé et d'invalidité. L'agence gouvernementale utilise le système de numérotation INSA pour enregistrer les patients et le système IPH pour enregistrer les praticiens de la santé afin de s'assurer que ces enregistrements sont précis tout en protégeant la confidentialité des individus. Cette règle détecte les numéros de la Personne commune de l'IPH de Nouvelle Zélande à 6 caractères alphanumériques (IPH-PCN), qui identifient de façon unique un travailleur ou un praticien de la santé. Cette règle détecte également les numéros INSA à 7 caractères utilisés pour identifier de façon unique un patient du système de santé néo-zélandais.

La règle cherche une correspondance dans n'importe quel commutateur de contenu :

- numéro de l'Indice des praticiens de la santé en Nouvelle-Zélande
- Numéro de l'Indice National de la Santé en Nouvelle-Zélande

Ohio HB-104

La loi d'état de protection des données Ohio HB-104 vise à protéger les informations personnellement identifiables. Approuvée le 17 novembre 2005 et entrée en vigueur le 29 décembre 2006, elle s'applique à tout individu, société, fiducie commerciale, patrimoine, société en fiducie, partenariat ou association qui conduit des affaires dans l'Ohio et détient ou certifie des données informatiques qui comprennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Oklahoma HB-2357

La loi d'état de protection des données Oklahoma HB-2357 vise à protéger les informations personnellement identifiables. Approuvée le 8 juin 2006 et entrée en vigueur le 1er novembre 2008, elle s'applique à toutes les sociétés, fiducies commerciales, patrimoines, partenariats, sociétés en commandite simple, sociétés de personnes à responsabilité limitée, sociétés à responsabilité limitée, associations, organisations, sociétés en participations, gouvernements, sections gouvernementales, agences ou intermédiaires, ou toute autre entité légale, avec ou sans but lucratif qui fait des affaires en Oklahoma HB-2357 et détient ou certifie des données informatisées non cryptées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros d'identification des patients

Les informations personnellement identifiables (IPI) communément détenues par les hôpitaux et les organisations et métiers en lien avec la santé aux États-Unis d'Amérique. Cette règle doit être personnalisée pour définir le format du numéro d'identification du patient.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéros d'identification des patients
- Numéro d'identification nationale de fournisseurs américains
- Numéro de sécurité sociale américain

Norme de sécurité informatique des données de l'industrie des cartes de paiement (PCI-DSS)

La norme PCI DSS, ensemble d'exigences détaillées pour l'amélioration de la sécurité informatique des données de compte de paiement, a été développée par les marques de paiement fondatrices du PCI Security Standards Council (PCI SSC), comprenant American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. International, afin de faciliter la large adoption de mesures de sécurité des données cohérentes sur une base globale.

La norme PCI DSS est une norme de sécurité multi-facettes qui comprend les exigences de gestion de la sécurité, des politiques, procédures, architecture réseau, conception logicielle et autres mesures de protection critiques. Cette norme détaillée a pour but d'aider les organisations à protéger de manière active les données de compte client.

La règle cherche au moins une correspondance dans n'importe quelle lame d'analyse de contenu :

- Numéro de carte de crédit
- Données de piste de carte de crédit

Texas SB-122

La loi d'état de protection des données Texas SB-122 vise à protéger les informations personnellement identifiables. Approuvée le 17 juin 2005 et entrée en vigueur le 1er septembre 2005, elle s'applique à toute personne qui fait des affaires au Texas et détient ou certifie des données informatisées non cryptées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Numéros BIC du Royaume-Uni

Le code d'identification des banques (BIC) identifie de façon unique une banque en particulier. Il est utilisé au Royaume-Uni et à l'échelle internationale afin de permettre l'échange d'argent et de messages entre banques. La politique identifie les documents et les transmissions qui contiennent des codes BIC, également connus sous le nom de codes SWIFT, émis par la SWIFT (Société des télécommunications mondiales financières interbancaires – Society for Worldwide Interbank Financial Telecommunication).

La règle cherche une correspondance dans la lame d'analyse de contenu du numéro BIC du Royaume-Uni.

Numéros de permis de conduire du Royaume-Uni

Le numéro de permis de conduire du Royaume-Uni est un numéro d'identification sur un permis de conduire du Royaume-Uni qui identifie le propriétaire dudit numéro pour la conduite et toute infraction au code de la route.

La règle cherche une correspondance dans la lame d'analyse de contenu du numéro de permis de conduire du Royaume-Uni.

Numéros IBAN du Royaume-Uni

Le numéro IBAN est une norme internationale d'identification des comptes bancaires au Royaume-Uni à travers les frontières nationales, adoptée au départ par le Comité européen des normes bancaires. Le registre officiel IBAN dans le cadre de l'ISO 13616:2003 est publié par la SWIFT (Société des télécommunications mondiales financières interbancaires – Society for Worldwide Interbank Financial Telecommunication).

La règle cherche une correspondance dans la lame d'analyse de contenu du numéro IBAN du Royaume-Uni.

Numéros du Service national de santé (NHS) du Royaume-Uni

Le numéro du Service national de santé du Royaume-Uni est un numéro d'identification fourni par le Service National de Santé du Royaume-Uni qui identifie le propriétaire dudit numéro à des fins de dossiers médicaux.

La règle cherche une correspondance dans la lame d'analyse de contenu du numéro du Service national de santé du Royaume-Uni.

Numéros d'assurance nationaux du Royaume-Uni

L'Assurance Sociale du Royaume-Uni est un système de paiements issus des gains des employés, des employeurs et des professions libérales au Gouvernement qui octroie une pension d'état et d'autres avantages.

Les numéros d'assurance nationaux du Royaume-Uni sont les numéros d'identification assignés à toute personne née au Royaume-Uni, ou à toute personne résidant au Royaume-Uni qui est un employé légal, étudiant, bénéficiaire de l'allocation sociale, pension, etc.

La règle cherche une correspondance, au moins d'une des lames d'analyse de contenu des numéros d'assurance nationaux formels du Royaume-Uni ou des numéros d'assurance nationaux informels du Royaume-Uni.

Numéros de passeport du Royaume-Uni

La règle identifie les documents et les transmissions qui contiennent les numéros de passeport émis au Royaume-Uni.

La règle cherche une correspondance parmi les numéros de passeport du Royaume-Uni dans la lame d'analyse de contenu.

Numéros de permis de conduire américains

Les permis de conduire émis aux États-Unis ont un numéro ou un code alphanumérique délivrés par le Département des véhicules à moteur (ou équivalent). Ils comportent habituellement une photo du détenteur, ainsi qu'une copie de sa signature, son adresse de résidence principale, le type ou la classe de permis, les restrictions et/ou contraventions (si applicable), les caractéristiques physiques du détenteur (telles que taille, poids, couleur des cheveux, des yeux et parfois même couleur de peau) et la date de naissance. Les numéros de permis émis par un état sont uniques. Les problèmes de vol d'identité conduisent à la disparition progressive des numéros de sécurité sociale devenant moins courants sur les permis de conduire.

La règle recherche une correspondance dans la lame d'analyse de contenu des permis américains.

Numéros de sécurité sociale américains

Le numéro de sécurité sociale américaine est émis pour les citoyens américains, les résidents permanents et les résidents temporaires (qui travaillent) selon la section 205(c)(2) de l'Acte de la sécurité sociale, sous le code 42 U.S.C. § 405(c)(2). Ce numéro est émis pour un individu par l'Administration de la sécurité sociale, agence indépendante du gouvernement des États-Unis. Son objectif principal est de suivre les individus à des fins fiscales.

Utah SB-69

La loi d'état de protection des données Utah SB-69 vise à protéger les informations personnellement identifiables. Approuvée le 20 mars 2006 et entrée en vigueur le 1er janvier 2007, elle s'applique à quiconque détient ou certifie des données informatisées qui comprennent des informations personnellement identifiables d'un résident de l'Utah.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Vermont SB-284

La loi d'état de protection des données Vermont SB-284 vise à protéger les informations personnellement identifiables. Approuvée le 18 mai 2006 et entrée en vigueur le 1er janvier 2007, elle s'applique à tout collecteur de données qui détient ou certifie des données informatisées non cryptées comprenant des informations personnellement identifiables d'un individu résidant dans le Vermont.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Washington SB-6043

La loi d'état de protection des données Washington SB-6043 vise à protéger les informations personnellement identifiables. Approuvée le 10 mai 2005 et entrée en vigueur le 24 juillet 2005, elle s'applique à tout état ou agence locale ou toute personne ou société qui fait des affaires à Washington et détient ou certifie des données informatisées qui contiennent des informations personnellement identifiables.

La politique recherche au moins une correspondance avec des informations personnellement identifiables, qui peuvent inclure les éléments suivants :

- Numéro de carte de crédit
- Données de piste de carte de crédit
- Numéro de permis de conduire américain
- Numéro de sécurité sociale américain

Lames d'analyse de contenu disponibles

Cette section répertorie les lames d'analyse de contenu disponibles pour les réglementations vShield.

Lame d'analyse de contenu de numéro de routage ABA

La lame d'analyse de contenu recherche les correspondances de 3 éléments d'information très proches l'un de l'autre.

La lame d'analyse de contenu recherche :

- Le numéro de routage ABA
- Les mots et expressions bancaires (par exemple, aba, numéro de routage, compte chèque courant, comptes d'épargne)
- Les informations personnellement identifiables (par exemple, nom, adresse, numéro de téléphone)

Les mots et expressions relatifs à la banque sont implémentés afin d'améliorer la précision. Un numéro de routage comporte 9 chiffres et peut se substituer à plusieurs types de données différents, par exemple, un numéro de sécurité sociale américain, d'assurance sociale canadien ou de téléphone international valides.

Étant donné que les numéros de routage eux-mêmes ne sont pas des informations sensibles, des renseignements personnellement identifiables sont nécessaires pour qu'une violation se produise.

Lame d'analyse de contenu « Dates d'admission et d'autorisation de sortie »

La lame d'analyse de contenu recherche les correspondances avec l'entité Format de date américain et les mots et expressions tels que date d'admission, date d'autorisation de sortie, très proches l'un de l'autre.

Lame d'analyse de contenu « Permis de conduire de l'État d'Alabama »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Alabama et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, des termes tels que AL ou Alabama.

Modèle du numéro de permis de conduire

7 ou 8 chiffres

Lame d'analyse de contenu « Permis de conduire de l'État d'Alaska »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Alaska et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, les termes tels que AK ou Alaska.

Modèle du numéro de permis de conduire :

7 chiffres

Lame d'analyse de contenu « Permis de conduire de la Province d'Alberta »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Alaska et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, les termes tels que AK ou Alaska.

Modèle du numéro de permis de conduire

7 chiffres

Lame d'analyse de contenu « Permis de conduire de l'État d'Alaska »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Alaska et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, les termes tels que AK ou Alaska.

Modèle du numéro de permis de conduire :

7 chiffres

Lame d'analyse de contenu « Permis de conduire de la Province d'Alberta »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Alaska et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, les termes tels que AK ou Alaska.

Modèle du numéro de permis de conduire

7 chiffres

Lame d'analyse de contenu « American Express »

La lame d'analyse de contenu recherche la combinaison des informations suivantes.

- Plus d'un numéro de carte de crédit American Express
- Un seul numéro de carte de crédit et les mots et expressions tels que ccn, carte de crédit, date d'expiration
- Un seul numéro de carte de crédit et une date d'expiration

Lame d'analyse de contenu « Permis de conduire de l'État d'Arizona »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Arizona et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, les termes tels que AZ ou Arizona.

Le modèle du numéro de permis de conduire peut être un caractère alphabétique, 8 ou 9 chiffres (numéro de sécurité sociale – SSN) ou 9 chiffres (SSN non formaté).

Lame d'analyse de contenu « Permis de conduire de l'État de l'Arkansas »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État d'Arkansas et les mots et expressions tels que permis de conduire et numéro de permis et, éventuellement, les termes tels que AR ou Arkansas.

Le modèle du numéro de permis de conduire peut être 9 ou 8 chiffres.

Lame d'analyse de contenu « Numéro de compte bancaire australien »

Le numéro de compte bancaire australien n'est pas lui-même sensible, mais identifie un compte bancaire, tout en n'identifiant pas la succursale de la banque. Par conséquent, le numéro de compte et les informations de la succursale doivent exister pour que le document soit considéré comme sensible.

La lame d'analyse de contenu recherche les correspondances avec les deux éléments d'information suivants :

- Un numéro de compte bancaire australien
- Des mots et des expressions relatives à la succursale d'état de la banque ou BSB.

Elle utilise également une règle d'expression ordinaire pour différencier les numéros de téléphone de même longueur.

Un numéro de compte bancaire australien comporte de 6 à 10 chiffres sans signification particulière intégrée. Il n'a pas de chiffre de contrôle.

Lame d'analyse de contenu « ABN (numéro d'entreprise australien) »

La lame d'analyse de contenu recherche les correspondances avec deux éléments d'information très proches l'un de l'autre.

- numéro d'entreprise australien
- Mots et expressions relatifs à ABN (par exemple, ABN, numéro d'entreprise australien)

Lame d'analyse de contenu « ACN (numéro de société australien) »

La lame d'analyse de contenu recherche les correspondances avec deux éléments d'information très proches l'un de l'autre.

- numéro de société australien
- Mots et expressions relatifs à ACN (par exemple, ACN, numéro de société australien)

Lame d'analyse de contenu « Numéro de carte Medicare australienne »

La lame d'analyse de contenu donne une correspondance si l'une des combinaisons suivantes d'éléments d'information apparaît dans un document.

- Plus d'un numéro de carte Medicare australienne
- Un numéro de carte Medicare australienne ou des termes d'identification du patient (par exemple, identificateur du patient, numéro du patient)
- Un numéro de carte Medicare plus deux éléments d'information parmi : un nom, une date d'expiration ou des termes d'expiration

Lame d'analyse de contenu « Numéro de dossier fiscal australien »

La lame d'analyse de contenu recherche les correspondances avec deux éléments d'information extrêmement proches l'un de l'autre.

- Numéro fiscal australien (voir la description de la personne morale)
- Mots et expressions relatifs au numéro de dossier fiscal (par exemple, TFN, numéro de dossier fiscal)

Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Californie »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État de Californie et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que CA ou California.

Le modèle du permis de conduire est 1 caractère alphabétique, 7 chiffres.

Lame d'analyse de contenu « Numéro de permis de conduire canadien »

La lame d'analyse de contenu est seulement un fichier conteneur pour les lames de contenu enfants. Les lames d'analyse de contenu qui lui sont assignées recherchent séparément les permis de conduire dans les provinces et territoires individuels.

Lame d'analyse de contenu « Numéro d'assurance sociale canadienne »

La lame d'analyse de contenu est seulement un fichier conteneur pour les lames de contenu enfants. Les lames d'analyse de contenu qui lui sont assignées recherchent séparément les versions mises en forme et non mises en forme des numéros d'assurance sociale canadienne ainsi que les informations personnelles afin que différentes règles puissent leurs être attribuées. La version mise en forme du numéro d'assurance sociale est un modèle plus spécifique et les règles de renvoi d'une correspondance sont donc moins strictes. Cependant, la version non mise en forme est très générale et correspond à de nombreux numéros communs.

Lame d'analyse de contenu « Numéro de permis de conduire de l'État du Colorado »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État de Colorado et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que CO ou Colorado.

Le modèle du numéro du permis de conduire est 9 chiffres.

Lame d'analyse de contenu « Numéro de permis de conduire de l'État du Connecticut »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État de Connecticut et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que CT ou Connecticut.

Modèle du numéro de permis de conduire : 9 chiffres, les deux premières positions correspondent au mois de naissance en année paire ou impaire. 01-12 Jan-Déc années impaires, 13-24 Jan-Déc années paires, 99 inconnu.

Lame d'analyse de contenu « Numéro de carte de crédit »

La lame d'analyse de contenu recherche la combinaison des informations suivantes.

- Plus d'un numéro de carte de crédit
- Un seul numéro de carte de crédit et les mots et expressions tels que ccn, carte de crédit, date d'expiration
- Un seul numéro de carte de crédit et une date d'expiration

Lame d'analyse de contenu « Données de piste de carte de crédit »

Les données de piste sont des informations codées et stockées sur deux pistes situées dans la bande magnétique au dos d'une carte de crédit (carte de paiement, carte cadeau, etc.). Il y a trois pistes sur la magstripe (bande magnétique au dos d'une carte de crédit).

Chaque piste mesure 2,8 mm (0,110 pouce) de large. La norme ISO/IEC 7811, qui est utilisée par les banques, stipule que :

- La piste n°1 a une densité d'enregistrement de 210 bits par pouce (bpi), et contient 79 caractères en lecture seule, chacun avec un codage sur six bits plus un bit de parité.
- La piste n°2 a une densité d'enregistrement de 75 bpi, et contient 40 caractères chacun avec un codage sur quatre bits plus un bit de parité.

- La piste n°3 a une densité d'enregistrement de 210 bpi et contient 107 caractères chacun avec un codage sur quatre bits plus un bit de parité.

Votre carte de crédit n'utilise généralement que les pistes n°1 et n°2. La piste n°3 est une piste pour lecture/écriture (qui inclut un numéro d'identification personnel (PIN) chiffré, le code du pays, les unités de devise, le montant autorisé), mais son utilisation n'est pas normalisée entre les banques.

Cette lame d'analyse de contenu nécessite une correspondance avec l'entité « Données de piste de carte de crédit ».

Lame d'analyse de contenu « Numéro de compte personnalisé »

La lame d'analyse de contenu « compte personnalisé » est une lame modifiable et doit contenir une expression ordinaire pour les modèles de compte personnalisé d'une organisation.

Lame d'analyse de contenu « Numéro de permis de conduire de l'État du Delaware »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État du Delaware et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que DE ou Delaware.

Lame d'analyse de contenu « Numéro de carte de paiement de l'UE »

La lame d'analyse de contenu recherche les modèles des principaux numéros de carte de paiement de l'Union Européenne.

La lame d'analyse de contenu recherchera des correspondances avec l'une ou l'autre combinaison des éléments d'information suivants à proximité immédiate :

- plus d'une correspondance avec un numéro de carte de paiement de l'UE
- une seule correspondance avec un numéro de carte de paiement de l'UE plus deux éléments parmi : un mot ou une expression pour une carte de crédit (par exemple, numéro de carte ou cc#), un code de sécurité de carte de crédit, une date d'expiration ou un nom
- une seule correspondance avec un numéro de carte de paiement de l'UE avec une date d'expiration

Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Floride »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État de Floride et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que FL ou Florida.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 12 chiffres.

Lame d'analyse de contenu « Numéro de permis de conduire français »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un permis de conduire français.

- Modèle d'un permis de conduire français
- Des mots ou des expressions pour un permis de conduire (par exemple, permis, permis de conduire) ou un format de date de l'U.E.

Lame d'analyse de contenu « Numéro BIC France »

La lame d'analyse de contenu exige des correspondances pour les deux règles suivantes lors de la recherche des numéros BIC français.

- Format de numéro BIC européen
- Format français du numéro BIC

Lame d'analyse de contenu « Numéro IBAN français »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro IBAN français.

- Format de numéro IBAN européen
- Modèle du numéro IBAN français

Lame d'analyse de contenu « Numéro d'identification national français »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro d'identification national français.

- Plus d'une correspondance avec le modèle de l'identification nationale française
- Une correspondance avec le modèle d'identification nationale française plus des mots ou des expressions d'un numéro de sécurité sociale

Lame d'analyse de contenu « Numéro français de TVA »

La lame d'analyse de contenu nécessite une correspondance pour un modèle de numéro français de TVA (taxe à la valeur ajoutée) tout près de l'abréviation FR.

Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Géorgie »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État de Georgie et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que GA ou Georgia.

Modèle du numéro de permis de conduire : 7 à 9 chiffres ; ou SSN mis en forme.

Lame d'analyse de contenu « Numéro BIC allemand »

La lame d'analyse de contenu exige des correspondances pour les deux règles suivantes lors de la recherche des numéros BIC allemands.

- Format de numéro BIC européen
- Format allemand du numéro BIC

Lame d'analyse de contenu de numéro de permis de conduire en Allemagne

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un permis de conduire allemand.

- Modèle du permis de conduire allemand \
- Mots ou expressions liés à un permis de conduire (par exemple, permis de conduire, ausstellungsdatum)

Lame d'analyse de contenu « Numéro IBAN allemand »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro IBAN allemand.

- Format de numéro IBAN européen
- Modèle du numéro IBAN allemand

Règle pour l'IBAN allemand : Code du pays « DE » suivi de 22 chiffres.

Lame d'analyse de contenu « Numéros d'identification nationaux allemands »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro d'identification national allemand.

- Soit un numéro d'identification national allemand, soit une version du numéro lisible par une machine
- Des mots ou des expressions pour un numéro d'identification national allemand (par exemple, personalausweis, personalausweisnummer)

Lame d'analyse de contenu « Numéro de passeport allemand »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro de passeport allemand.

- Soit un numéro de passeport allemand, soit une version du numéro lisible par une machine
- Des mots ou des expressions pour un numéro de passeport allemand ou une date de délivrance (par exemple, reisepass, ausstellungsdatum)

Lame d'analyse de contenu « Numéro de TVA allemand »

La lame d'analyse de contenu nécessite une correspondance pour un modèle de numéro allemand de TVA (voir la description de l'entité) tout près de l'abréviation DE.

Lame d'analyse de contenu « Numéros d'assurance de groupe »

Cette lame d'analyse de contenu nécessite une personnalisation. Pour utiliser cette lame d'analyse de contenu, ajoutez une expression ordinaire pour une correspondance avec le modèle du numéro d'assurance de groupe d'une organisation. La lame d'analyse de contenu recherche des mots et des expressions tels que « assurance de groupe » ou un nom, une adresse ou une date américaine en combinaison avec l'expression ordinaire personnalisée.

Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Hawaii »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'État de Hawaii et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que HI ou Hawaii.

Modèle du numéro de permis de conduire : Caractère alphabétique H, 8 chiffres ; ou SSN.

Lame d'analyse de contenu « Numéros d'identification nationaux en Italie »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro d'identification national italien.

1 Modèle du Numéro d'identification national italien

2 Mots ou expressions pour un numéro d'identification national italien (par exemple, codice fiscale, identification nationale)

Règle pour l'identification nationale : Code à 16 caractères alphanumériques, où :

- *SSS* sont les trois premières consonnes du nom de famille (la première voyelle puis un X est utilisé s'il n'y a pas suffisamment de consonnes)
- *NNN* sont la première, la troisième et la quatrième consonne du prénom ; les exceptions sont traitées comme pour les noms de famille
- *YY* sont les derniers chiffres de l'année de naissance
- *M* est la lettre correspondant au mois de naissance – les lettres sont utilisées dans l'ordre alphabétique, mais seules les lettres A à E, H, L, M, P, R à T sont utilisées (ainsi, janvier est A et octobre est R)
- *DD* est le jour du mois de naissance – pour différencier les sexes, 40 est ajouté au jour de naissance pour les femmes (ainsi, une femme née le 3 mai a ...E43...)
- *ZZZZ* est un code géographique spécifique à la municipalité où la personne est née – les codes à l'échelle nationale sont utilisés pour les pays étrangers, une lettre suivie de trois chiffres
- *X* est un caractère de parité calculé en ajoutant les caractères des positions paires et impaires, et en divisant par 26. Des valeurs numériques sont utilisées pour les lettres dans les positions paires en fonction de leur ordre alphabétique. Les caractères dans des positions impaires ont différentes valeurs. Une lettre est alors utilisée et correspond à la valeur du reste de la division dans l'alphabet.

Modèle :

- *LLLLLLDDLDDLDDDL*
- *LLL LLL DDLDD LDDDL*

Numéros des bénéficiaires du régime de soins médicaux

Cette lame d'analyse de contenu nécessite une personnalisation. Pour utiliser cette lame d'analyse de contenu, ajoutez une expression ordinaire de façon à identifier les bénéficiaires des indemnités et versements du régime de soins médicaux. La lame d'analyse de contenu recherche des mots et des expressions tels que « bénéficiaire » ou un nom, une adresse ou une date américaine en combinaison avec l'expression ordinaire personnalisée.

Lame d'analyse de contenu « Numéro de permis de conduire de l'état d'Idaho »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'état de l'Idaho et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que ID ou Idaho.

Modèle du numéro de permis de conduire : 2 caractères alphabétiques, 6 chiffres, 1 caractère alphabétique.

Lame d'analyse de contenu « Numéro de permis de conduire de l'état de l'Illinois »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'état de l'Illinois et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que IL ou Illinois.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 11 chiffres.

Lame d'analyse de contenu « Numéro de permis de conduire de l'état de l'Indiana »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'état de l'Indiana et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que IN ou Indiana.

Modèle du numéro de permis de conduire : 10 chiffres.

Lame d'analyse de contenu « Numéro de permis de conduire de l'état de l'Iowa »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'état de l'Iowa et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que IA ou Iowa.

Le modèle du numéro de permis de conduire peut comporter 3 chiffres, 2 caractères alphabétiques, 3 chiffres ; ou le Numéro de sécurité sociale.

Lame d'analyse de contenu « Index des Procédures »

La lame d'analyse de contenu recherche des mots et des expressions relatives aux procédures médicales basées sur la Classification internationale des maladies (International Classification of Diseases – ICD).

La lame d'analyse de contenu recherchera des correspondances avec une combinaison des éléments d'information suivants, si :

- il existe plus d'une correspondance avec le dictionnaire Index des Procédures
- il existe une seule correspondance avec le dictionnaire Index des Procédures plus deux éléments d'information parmi : un nom, une adresse américaine ou une date américaine
- il existe une seule correspondance avec le dictionnaire Index des Procédures plus un mot ou une expression identifiant un patient ou un médecin (par exemple, ID du patient, nom du médecin)

Lame d'analyse de contenu « Numéro de permis de conduire italien »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un permis de conduire italien.

- Modèle du permis de conduire italien
- Mots ou expressions pour un permis de conduire (par exemple, permis de conduire, patente di guida)

Règle pour le permis de conduire : 10 caractères alphanumériques -- 2 lettres, 7 chiffres et une dernière lettre. La première lettre peut être uniquement un caractère entre A et V.

Modèle du permis de conduire :

- *LLDDDDDDDL*
- *LL DDDDDDD* L
- *LL-DDDDDDD-L*
- *LL - DDDDDDD - L*

Lame d'analyse de contenu « Numéro IBAN italien »

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro IBAN italien.

1 Mots et expressions relatifs à un IBAN (par exemple, Compte bancaire international, IBAN)

2 Modèle du numéro IBAN italien

Règle pour IBAN : Code du pays `IT` suivi de 25 caractères alphanumériques.

Modèle :

- `IT`*DDLDDDDDDDDDDAAAAAAAAAAA*
- `IT` *DDL DDDDD DDDDD AAAAAAAAAAA*
- `IT` *DD LDDDDD DDDDD AAAAAAAAAAA*

- IT *DD L DDDDD DDDDD AAAAAAAAAAAA*
- IT *DD LDDDDDDDDDDAAAAAAAAAAAA*
- IT *DD L DDDDDDDDDDAAAAAAAAAAAA*
- IT*DD LDDD DDDD DDDA AAAA AAAA AAA*
- IT *DDL DDDDD DDDDD AAAAAA AAAAAA*
- IT *DDL DDD DDD DDD DAAA AAA AAAAAA*
- IT *DDL DDDDDDDDDD AAAAAA AAAAAA*

Les espaces peuvent être remplacés par des tirets, barres obliques ou deux points.

Lame d'analyse de contenu « ITIN non mis en forme »

La lame d'analyse de contenu recherche des modèles non mis en forme du Numéro d'identification du contribuable (ITIN) américain. La lame d'analyse de contenu donne une correspondance si un ITIN non mis en forme est trouvé tout près d'un mot ou d'une expression pour un numéro ITIN (par exemple, identification fiscale, ITIN).

Règle pour ITIN : Un nombre à neuf chiffres qui commence toujours par le chiffre 9 et dont le quatrième et le cinquième chiffre sont compris dans une plage de numéros de 70 à 88.

Modèle : *DDDDDDDDD*

Lame d'analyse de contenu « Numéro de permis de conduire de l'état du Kansas »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'état du Kansas et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que KS ou Kansas.

Modèle du numéro de permis de conduire : 1 caractère alphabétique (K), 8 chiffres ; ou le Numéro de sécurité sociale.

Lame d'analyse de contenu « Numéro de permis de conduire de l'état du Kentucky »

La lame d'analyse de contenu recherche les correspondances entre le modèle du permis de conduire de l'état du Kentucky et les mots et expressions tels que permis de conduire et numéro de permis et les termes tels que KY ou Kentucky.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 8 chiffres ; ou le Numéro de sécurité sociale.

Lame d'analyse de contenu des numéros de permis de conduire de Louisiane

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Louisiane et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que LA ou Louisiane.

Modèle du numéro de permis de conduire : 2 zéros, 7 chiffres.

Lame d'analyse de contenu des numéros de permis de conduire du Maine

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Maine et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que ME ou Maine.

Modèle du numéro de permis de conduire : 7 chiffres, caractère alphabétique X facultative.

Lame d'analyse de contenu des permis de conduire du Manitoba

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Manitoba et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que MB ou Manitoba.

Règles de modèle du numéro de permis : 12 caractères alphanumériques qui peuvent être séparés par un trait d'union, où :

- le 1er caractère est une lettre
- du 2ème au 5ème, les caractères sont une lettre ou un astérisque
- le 6ème caractère est une lettre
- du 7ème au 10ème, les caractères sont des chiffres
- le 11ème caractère est une lettre
- le 12ème caractère est une lettre ou un chiffre

ou

- le 1er caractère est une lettre
- du 2ème au 4ème, les caractères sont une lettre ou un astérisque
- les 5ème et 6ème caractères sont des chiffres
- du 7ème au 12ème, les caractères sont une lettre ou un chiffre

Modèle du numéro de permis de conduire :

- *LLLLLLDDDDLA*
- *LLLLLDDAAAAAA*

Lame d'analyse de contenu des numéros de permis de conduire du Maryland

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Maryland et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MD ou Maryland.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 12 chiffres

Lame d'analyse de contenu des numéros de permis de conduire du Massachusetts

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Massachusetts et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MA ou Massachusetts.

Modèle du numéro de permis de conduire : 1 caractère alphabétique (S), 8 chiffres ; ou numéro de sécurité sociale

Lame d'analyse de contenu des numéros de permis de conduire du Michigan

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Michigan et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MI ou Michigan.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 12 chiffres

Lame d'analyse de contenu des numéros de permis de conduire du Minnesota

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Minnesota et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MN ou Minnesota

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 12 chiffres

Lame d'analyse de contenu des numéros de permis de conduire du Mississippi

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Mississippi et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MS ou Mississippi.

Modèle du numéro de permis de conduire : 9 chiffres ; ou numéro de sécurité sociale formaté

Lame d'analyse de contenu des numéros de permis de conduire du Missouri

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Missouri et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MO ou Missouri.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 6-9 chiffres ; ou 9 chiffres ; ou numéro de sécurité sociale formaté

Lame d'analyse de contenu des numéros de permis de conduire du Montana

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Montana et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que MT ou Montana.

Modèle du numéro de permis de conduire : 9 chiffres (SSN) ; ou 1 caractère alphabétique, 1 chiffre, 1 alphanumérique, 2 chiffres, 3 caractères alphabétiques et 1 chiffre ; ou 13 chiffres

Lame d'analyse de contenu des dictionnaires de formules du code national de drogue (NDC)

La lame d'analyse de contenu cherche les mots et expressions en relation avec les formules basées sur les Codes nationaux de drogue (NDC).

La lame d'analyse de contenu recherchera des correspondances avec une combinaison des éléments d'information suivants, si :

1 Plus d'une correspondance avec le dictionnaire des formules du NDC

2 Une seule correspondance avec le dictionnaire de formules du NDC, plus deux correspondances soit un nom, une adresse américaine ou une date américaine

3 Une seule correspondance avec le dictionnaire de formules du NDC avec un mot ou une expression pour l'identification patient ou médecin (par exemple, ID patient, nom du médecin)

Lame d'analyse de contenu des numéros de permis de conduire du Nebraska

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Nebraska et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NE ou Nebraska.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 8 chiffres

Lame d'analyse de contenu des numéros de permis de conduire des Pays-Bas

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un permis de conduire des Pays-Bas.

1 Modèle de permis de conduire des Pays-Bas (consulter la description de l'entité)

2 Mots ou expressions pour un permis de conduire (par exemple, permis de conduire, rijbewijs)

Lame d'analyse de contenu des numéros IBAN des Pays-Bas

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro IBAN des Pays-Bas.

1 Mots et expressions relatifs à un IBAN (par exemple, Compte bancaire international, IBAN)

2 Modèle de numéro IBAN des Pays-Bas

Règle pour IBAN : Code pays `NL` suivi de 16 caractères alphanumériques.

Modèle :

- `NL`*DDLLLLDDDDDDDDDD*
- `NL` DDLLLLDDDDDDDDDD
- `NL` *DD LLLL DDDDDDDDDD*
- `NL` *DD LLLL DDDD DDDD DD*
- `NL`*DD LLLL DDDD DDDD DD*
- `NL`*DDLLLL DDDD DDDDDD*
- `NL`*DD LLLL DDDDDDDDDD*
- `NL` DD LLLL D DD DD DD DDD
- `NL` *DD LLLL DD DD DD DDDD*
- `NL` *DD LLLL DDD DDDDDDD*
- `NL` *DD LLLL DDDD DD DD DD*

Les espaces peuvent être remplacés par des tirets

Lame d'analyse de contenu des numéros d'identification nationale des Pays-Bas

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro d'identification nationale des Pays-Bas.

1 Numéro d'identification nationale des Pays-Bas (consulter la description de l'entité)

2 Mots ou expressions pour un numéro d'identification nationale des Pays-Bas (par exemple, sofinummer, burgerservicenummer)

Lame d'analyse de contenu des numéros de passeport des Pays-Bas

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro de passeport des Pays-Bas.

1 Numéro de passeport des Pays-Bas (consulter la description de l'entité)

2 Mots ou expressions pour un numéro de passeport des Pays-Bas (par exemple, paspoort, Noodpaspoort)

Lame d'analyse de contenu des numéros de permis de conduire du Nevada

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Nevada et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NV ou Nevada.

Modèle du numéro de permis de conduire : 9 chiffres (SSN) ; ou 12 chiffres (les 2 derniers sont l'année de naissance), ou 10 chiffres

[Lame d'analyse de contenu des permis de conduire du New Brunswick]

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du New Brunswick et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que NB ou New Brunswick.

Règles de modèle du numéro de permis : 5 - 7 chiffres

Modèle du numéro de permis de conduire :

- *DDDDD*
- *DDDDDD*
- *DDDDDDD*

Lame d'analyse de contenu des numéros de permis de conduire du New Hampshire

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du New Hampshire et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NH ou New Hampshire.

Modèle du numéro de permis de conduire : 2 chiffres, 3 caractères alphabétiques, 5 chiffres

Lame d'analyse de contenu des numéros de permis de conduire du New Jersey

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du New Jersey et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NJ ou New Jersey.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 14 chiffres

Lame d'analyse de contenu des numéros de permis de conduire du Nouveau-Mexique

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Nouveau-Mexique et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NM ou New Mexico.

Modèle du numéro de permis de conduire : 9 chiffres

Lame d'analyse de contenu des numéros de permis de conduire de l'état de New York

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'état de New York et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NY ou New York.

Modèle du numéro de permis de conduire : 9 chiffres

Lame d'analyse de contenu des indices des praticiens de la santé en Nouvelle-Zélande

La lame d'analyse de contenu cherche les correspondances entre l'entité Indices des praticiens de la santé en Nouvelle-Zélande et les termes qui corroborent comme hpi-cpn ou indice des praticiens de la santé.

Numéro de service des recettes fiscales de Nouvelle-Zélande

La lame d'analyse de contenu cherche les correspondances de l'entité Numéro de service des recettes fiscales de Nouvelle-Zélande et les mots et expressions tels que Numéro IRD ou Numéro de service des recettes fiscales.

Lame d'analyse de contenu des numéros de l'Indice National de la Santé en Nouvelle-Zélande

La lame d'analyse de contenu cherche les correspondances entre l'entité Indice national de la santé en Nouvelle-Zélande et les termes qui corroborent comme nhi-cpn ou indice national de la santé.

Lame d'analyse de contenu des permis de conduire de Terre-Neuve-et-Labrador

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Terre-Neuve-et-Labrador et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que NL ou Labrador.

Règles de modèle du numéro de permis : 1 lettre suivie de 9 chiffres

Modèle du numéro de permis de conduire : *LDDDDDDDDD*

Lame d'analyse de contenu des numéros de permis de conduire de Caroline du Nord

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Caroline du Nord et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que NC ou Caroline du Nord.

Modèle du numéro de permis de conduire : 6 - 8 chiffres

Lame d'analyse de contenu des numéros de permis de conduire du Dakota du Nord

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Dakota du Nord et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que ND ou Dakota du Nord.

Modèle du numéro de permis de conduire : 9 chiffres ; ou 3 caractères alphabétiques, 6 chiffres

Lame d'analyse de contenu des permis de conduire de la Nouvelle-Écosse

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de la Nouvelle-Écosse et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que NS ou Nouvelle-Écosse.

Règles de modèle du numéro de permis : 5 lettres suivies de 9 chiffres

Modèle du numéro de permis de conduire : *LLLLDDDDDDDDD*

Lame d'analyse de contenu des numéros de permis de conduire de l'Ohio

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'Ohio et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que OH ou Ohio.

Modèle du numéro de permis de conduire : 2 caractères alphabétiques, 6 chiffres

Lame d'analyse de contenu de numéro de permis de conduire de l'Oklahoma

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'Oklahoma et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que OK ou Oklahoma .

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 8 chiffres ; ou 9 chiffres ; ou numéro de sécurité sociale formaté

Lame d'analyse de contenu des permis de conduire de l'Ontario

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'Ontario et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que ON ou Ontario.

Règles de modèle du numéro de permis : 1 lettre suivie de 14 chiffres

Modèle du numéro de permis de conduire : *LDDDDDDDDDDDDD*

Lame d'analyse de contenu de numéro de permis de conduire de l'Oregon

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'Oregon et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que OR ou Oregon.

Modèle du numéro de permis de conduire : 6 -7 chiffres

Lame d'analyse de contenu des numéros d'identification des patients

Cette lame d'analyse de contenu nécessite une personnalisation. Pour utiliser cette lame d'analyse de contenu, ajoutez une expression courante pour un modèle de numéro d'identification des patients spécifique à une société. La lame d'analyse de contenu cherche des correspondances avec les mots et expressions tels qu'id patient ou nom, adresses américaines ou date américaine en combinaison avec l'expression courante personnalisée.

Lame d'analyse de contenu de numéro de permis de conduire de Pennsylvanie

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Pennsylvanie et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que PA ou Pennsylvanie.

Modèle du numéro de permis de conduire : 8 chiffres

Lame d'analyse de contenu des permis de conduire de l'Île-du-Prince-Édouard

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'Île-du-Prince-Édouard et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que PE ou Île-du-Prince-Édouard.

Règles de modèle du numéro de permis : 5 - 6 chiffres

Modèle du numéro de permis de conduire :

- *DDDD*
- *DDDDDD*

Lame d'analyse de contenu des conditions des informations protégées sur la santé

La lame d'analyse de contenu cherche des mots et des expressions en lien avec les dossiers de santé personnels et les réclamations d'assurance de santé.

La lame d'analyse de contenu recherchera des correspondances avec une combinaison des éléments d'information suivants, si :

1 Plus d'une correspondance avec le dictionnaire des informations protégées sur la santé

2 Une seule correspondance avec le dictionnaire des informations protégées sur la santé, plus deux correspondances soit d'un nom, d'une adresse américaine ou d'une date américaine

3 Une seule correspondance avec le dictionnaire des informations protégées sur la santé avec un mot ou une phrase d'identification d'un patient ou d'un médecin (c'est-à-dire ID patient, nom du médecin)

Lame d'analyse de contenu des permis de conduire du Québec

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Québec et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que QC ou Québec.

Règles de modèle du numéro de permis : 1 lettre suivie de 12 chiffres

Modèle du numéro de permis de conduire : LDDDDDDDDDDDD

Lame d'analyse de contenu de numéro de permis de conduire de Rhode Island

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Rhode Island et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que RI ou Rhode Island.

Modèle du numéro de permis de conduire : 7 chiffres

Lame d'analyse de contenu des permis de conduire de Saskatchewan

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Saskatchewan et les mots et expressions comme permis de conduire et numéro d'immatriculation ou les termes tels que SK ou Saskatchewan.

Règles de modèle du numéro de permis : 8 chiffres

Modèle de permis : *DDDDDDDD*

Lame d'analyse de contenu des numéros d'assurance sociale formatés

La lame d'analyse de contenu cherche les modèles formatés de numéros d'assurance sociale canadien.

La lame d'analyse de contenu concordera avec une combinaison des informations suivantes en proximité moyenne, soit :

1 plus d'une correspondance avec un numéro d'assurance sociale formaté

2 une seule correspondance avec un numéro d'assurance sociale formaté plus un mot ou une expression comme permis de conduire ou date de naissance

3 une seule correspondance avec un numéro d'assurance sociale avec mot ou e

Lame d'analyse de contenu des numéros d'assurance sociale non formatés

La lame d'analyse de contenu cherche les modèles non formatés de numéros d'assurance sociale canadien. La lame d'analyse de contenu concordera si un numéro d'assurance sociale non formaté est trouvé en proche proximité d'un mot ou d'une expression pour un numéro d'assurance sociale (par exemple, assurance sociale, SIN) ou un permis ou une date de naissance.

Lame d'analyse de contenu des numéros de sécurité sociale formatés

Lame d'analyse de contenu des numéros de sécurité sociale formatés

La lame d'analyse de contenu concordera avec une combinaison des informations suivantes en proximité moyenne, soit :

- Plus d'une correspondance avec un numéro de sécurité sociale formaté
- Une seule correspondance avec le dictionnaire de numéros de sécurité sociale formatés, plus deux correspondances soit d'un nom, d'une adresse américaine ou d'une date américaine
- Une seule correspondance avec le dictionnaire de numéros de sécurité sociale formatés avec un mot ou une expression pour un numéro de sécurité sociale (par exemple, Sécurité Sociale, SSN)

Lame d'analyse de contenu des numéros de sécurité sociale non formatés

La lame d'analyse de contenu cherche les modèles non formatés de numéros de sécurité sociale américaine (SSN). La lame d'analyse de contenu concordera si un SSN non formaté est trouvé en proche proximité d'un mot ou d'une expression pour un numéro de sécurité sociale (par exemple, Sécurité Sociale, SSN).

Lame d'analyse de contenu de numéro de permis de conduire de Caroline du Sud

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Caroline du Sud et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que SC ou Caroline du Sud.

Modèle du numéro de permis de conduire : 9 chiffres

Lame d'analyse de contenu de numéro de permis de conduire du Dakota du Sud

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Dakota du Sud et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que SD ou Dakota du Sud.

Modèle du numéro de permis de conduire : 8 chiffres ; ou numéro de sécurité sociale

Lame d'analyse de contenu des numéros d'identification nationale espagnols

La lame d'analyse de contenu cherche les correspondances entre l'entité du numéro d'identification nationale espagnol et les mots ou expressions tels que Documento Nacional de Identidad et Número de Identificación de Extranjeros. Elle utilise également les expressions courantes pour différencier les numéros de téléphone et pour éviter un double comptage des DNI et des NIE sans vérification des lettres.

Lame d'analyse de contenu des numéros de passeport espagnol

La lame d'analyse de contenu cherche les correspondances entre le numéro de passeport espagnol et les mots et expressions tels que pasaporte ou passeport.

Règle de passeport : 8 caractères alphanumériques : 2 lettres suivies de 6 chiffres.

Modèle :

LLDDDDDD

LL-DDDDDD

LL DDDDDD

Lame d'analyse de contenu des numéros de sécurité sociale espagnols

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro de sécurité sociale espagnol.

1 Numéro de sécurité sociale espagnol

2 Mots ou expressions pour un numéro de sécurité sociale (par exemple, número de la seguridad social, numéro de sécurité sociale)

Lame d'analyse de contenu des numéros IBAN suédois

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro IBAN suédois.

1 Mots ou expressions IBAN (par exemple, numéro de compte bancaire international, IBAN)

2 Modèle de numéro IBAN suédois

Règle pour IBAN : Code pays SE suivi de 22 chiffres.

Modèle : SE DDDDDDDDDDDDDDDDDDDDDD

Lame d'analyse de contenu des numéros de passeport suédois

La lame d'analyse de contenu cherche des correspondances entre l'expression courante Numéro de passeport suédois et les combinaisons possibles suivantes de justificatif.

1 Mots et expressions pour le passeport tels que le numéro de passeport

2 Mots et expressions pour la Suède, nationalité et date d'expiration

Règle de passeport : 8 chiffres

Modèle :

DDDDDDDD

DD-DDDDDD

LL-DDDDDD

Lame d'analyse de contenu de numéro de permis de conduire du Tennessee

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Tennessee et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que TX ou Tennessee.

Modèle du numéro de permis de conduire : 8 chiffres

Lame d'analyse de contenu des numéros BIC du Royaume-Uni

La lame d'analyse de contenu analyse les numéros BIC du Royaume-Uni en requérant des correspondances pour les deux règles.

1 Format de numéro BIC européen

2 Format du numéro BIC au Royaume-Uni

Règle BIC : 8 ou 11 caractères alphanumériques. Les lettres en 5ème et 6ème positions seront toujours « GB » selon le code ISO 3166-1 lettre -2 code pays.

Modèle :

LLLLLLAAA

LLLLLLAAAAA

LLLLLLAA-AAA

LLLLLLAA AAA

LLLLLL AA AAA

LLLL LL AA AAA

LLLL LL AA-AAA

Lame d'analyse de contenu des numéros de permis de conduire du Royaume-Uni

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un permis de conduire du Royaume-Uni.

1 Modèle de permis de conduire du Royaume-Uni

2 Soit les mots ou expressions pour un permis de conduire (par exemple, permis de conduire), soit l'identification personnelle (par exemple, date de naissance, adresse, téléphone)

Règle permis de conduire : 16 - 18 caractères alphanumériques commençant par une lettre.

Modèle :

LAAAADDDDDDLLDLLDD

Certains chiffres ont des valeurs limitées.

Lame d'analyse de contenu des numéros IBAN du Royaume-Uni

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro IBAN du Royaume-Uni.

1 Format de numéro IBAN européen

2 Modèle de numéro IBAN du Royaume-Uni

Règle pour IBAN : Code pays « GB » suivi de 20 caractères.

GB, code pays ISO

2 chiffres (caractères numériques de 0 à 9 seulement), chiffres de contrôle (IBAN)

4 lettres majuscules (A-Z uniquement), chiffres identificateurs de banque

6 chiffres (caractères numériques de 0 à 9 seulement), code guichet

8 chiffres (caractères numériques de 0 à 9 seulement), numéro de compte

Modèle :

GBDDLLLLDDDDDDDDDDDDDD

GB DD LLLL DDDD DDDD DDDD DD

GB DD LLLL DDDDDD DDDDDDDD

Lame d'analyse de contenu des numéros du Service national de santé du Royaume-Uni

La lame d'analyse de contenu requiert les choses suivantes pour rechercher une correspondance à proximité immédiate d'un numéro du Service national de santé du Royaume-Uni.

1 Format du numéro du Service national de santé du Royaume-Uni

2 Mots et expressions en lien avec le Service national de santé ou identification patient ou date de naissance

Lame d'analyse de contenu des numéros d'assurance nationaux formels du Royaume-Uni

La lame d'analyse de contenu cherche le modèle de format du numéro d'assurance national du Royaume-Uni.

La lame d'analyse de contenu concordera avec une combinaison des informations suivantes en proximité haute, soit :

1 plus d'une correspondance avec un modèle de numéro d'assurance national formel

2 Une seule correspondance entre les numéros d'assurance nationaux formels et un mot ou une expression pour un numéro d'assurance national (par exemple, NINO, numéro de contribuable)

Lame d'analyse de contenu des numéros de passeport du Royaume-Uni

La lame d'analyse de contenu cherche des correspondances entre l'une des entités des numéros de passeport du Royaume-Uni et le justificatif suivant.

1 Mots et expressions pour le passeport tels que passeport ou un code de passeport national précédant un numéro de passeport

2 Mots et expressions pour le pays, Royaume-Uni ou la date d'émission (correspondance optionnelle)

Lame d'analyse de contenu de numéro de permis de conduire de l'Utah

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'Utah et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que UT ou Utah.

Modèle du numéro de permis de conduire : 6 - 10 chiffres

Lame d'analyse de contenu de numéro de permis de conduire de Virginie

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de Virginie et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que VA ou Virginie.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 8 chiffres

Lame d'analyse de contenu des numéros de carte Visa

La lame d'analyse de contenu cherche une combinaison des éléments d'informations suivants, soit :

1 plus d'un numéro de carte de crédit JCB

2 Un seul numéro de carte de crédit et les mots et expressions tels que ccn, carte de crédit, date d'expiration

3 Un seul numéro de carte de crédit et une date d'expiration

Lame d'analyse de contenu de numéro de permis de conduire de Washington

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire de l'état de Washington et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que WA ou Washington.

Modèle du numéro de permis de conduire : 5 caractères alphabétiques (nom de famille), 1 caractère alphabétique (prénom), 1 caractère alphabétique (deuxième prénom), 3 chiffres, 2 alphanumériques. Si le champ du nom de famille ou du deuxième prénom est trop court, remplir avec des *.

Lame d'analyse de contenu de numéro de permis de conduire du Wisconsin

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Wisconsin et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que WI ou Wisconsin.

Modèle du numéro de permis de conduire : 1 caractère alphabétique, 13 chiffres

Lame d'analyse de contenu de numéro de permis de conduire du Wyoming

La lame d'analyse de contenu cherche les correspondances entre le modèle de permis de conduire du Wyoming et les mots et expressions comme permis de conduire et numéro de permis de conduire ou les termes tels que WY ou Wyoming.

Modèle du numéro de permis de conduire : 9 - 10 chiffres

Formats de fichier pris en charge

vShield Data Security peut détecter les formats de fichier suivants.

Tableau 13-2. Formats d'archive

Format d'application	Extensions
7-Zip 4.57	7Z
BinHex	HQX
BZIP2	BZ2
Expert Witness (EnCase)Compression Format	E0, E101 etc.
GZIP 2	GZ
ISO-9660 CD Disc Image Format	ISO
Java Archive	JAR
Legato EMailXtender Archive	EMX
MacBinary	BIN
Mac Disk copy Disk Image	DMG
Fichier de sauvegarde Microsoft	BKF

Tableau 13-2. Formats d'archive (suite)

Format d'application	Extensions
Microsoft Cabinet Format 1.3	CAB
Dossier compressé Microsoft	LZH LHA
Microsoft Entourage	
Microsoft Outlook Express	DBX
Microsoft Outlook Offline Store 2007	OST
Microsoft Outlook Personal Store 2007	PST
OASIS Open Document Forma	ODC SXC STC ODT SXW STW
Open eBook Publication Structure	EPUB
PKZIP	ZIP
RAR archive	RAR
Archives à extraction automatique	SEA
Shell Scrap Object File	SHS
Archive de bande	TAR
UNIX Compress	Z
UUEncoding	UUE
WinZip	ZIP

Tableau 13-3. Formats de CAO

Format d'application	Extensions
CATIA formats 5	CAT
Microsoft Visio 5, 2000, 2002, 2003, 2007	VSD
MicroStation 7, 8	DGN
Omni Graffle	GRAFFLE

Tableau 13-4. Formats de base de données

Format d'application	Extensions
Microsoft Access 95, 97, 2000, 2002, 2003, 2007	MDB

Tableau 13-5. Formats d'affichage

Format d'application	Extensions
Adobe PDF 1.1 à 1.7	PDF

Tableau 13-6. Formats de courriers électroniques

Format d'application	Extensions
Domino XML Language	DXL
Legato Extender	ONM
Lotus Notes database 4, 5, 6.0, 6.5, 7.0 et 8.0	NSF
Mailbox Thunderbird 1.0 et Eudora 6.2	MBX
Microsoft Outlook 97, 2000, 2002, 2003 et 2007	MSG
Microsoft Outlook Express Windows 6 et MacIntosh 5	EML
Microsoft Outlook Personal Folder 97, 2000, 2002 et 2003	PST
Text Mail (MIME)	Divers

Tableau 13-7. Formats multimédia

Format d'application	Extensions
Advanced Streaming Format 1.2	DXL

Tableau 13-8. Formats de présentation

Format d'application	Extensions
Apple iWork Keynote 2, 3, ‘08 et ‘09	GZ
Applix Presents 4.0, 4.2, 4.3, 4.4	AG
Corel Presentations 6, 7, 8, 9, 10, 11, 12 et X3	SHW
Lotus Freelance Graphics 2	PRE
Lotus Freelance Graphics 96, 97, 98, R9 et 9.8	PRZ
Macromedia Flash through 8.0	SWF
Microsoft PowerPoint PC 4	PPT
Microsoft PowerPoint Windows 95, 97, 2000, 2002 et 2003	PPT, PPS, POT
Microsoft PowerPoint Windows XML 2007	PPTX, PPTM, POTX, POTM, PPSX et PPSM
Microsoft PowerPoint Macintosh 98, 2001, v.X et 2004	PPT
OpenOffice Impress 1 et 1.1	SXP
StarOffice Impress 6 et 7	SXP

Tableau 13-9. Formats de feuille de calcul

Format d'application	Extensions
Apple iWork Numbers '08 et 2009	GZ
Applix Spreadsheets 4.2, 4.3 et 4.4	AS
Comma Separated Values	CSV
Corel Quattro Pro 5, 6, 7, 8, X4	WB2. WB3, QPW
Data Interchange Format	DIF
Lotus 1-2-3 96, 97, R9, 9.8, 2, 3, 4, 5	123, WK4
Lotus 1-2-3 Charts 2, 3, 4, 5	123
Microsoft Excel Windows 2.2 jusqu'à 2003	XLS, XLW, XLT, XLA

Tableau 13-9. Formats de feuille de calcul (suite)

Format d'application	Extensions
Microsoft Excel Windows XML 2007	XLSX, XLTX, XLSM, XLTM, XLAM
Microsoft Excel Charts 2, 3, 4, 5, 6, 7	XLS
Microsoft Excel Macintosh 98, 2001, v.X, 2004	XLS
Microsoft Office Excel Binary Format 2007	XLSB
Microsoft Works Spreadsheet 2, 3, 4	S30 S40
Oasis Open Document Format 1, 2	ODS, SXC, STC
OpenOffice Calc 1, 1.1	SXC, ODS, OTS
StarOffice Calc 6, 7	

Tableau 13-10. Formats texte et de balisage

Format d'application	Extensions
ANSI	TXT
ASCII	TXT
Extensible Forms Description Language	XFDL, XFD
HTML 3, 4	HTM, HTML
Microsoft Excel Windows XML 2003	XML
Microsoft Word Windows XML 2003	XML
Microsoft Visio XML 2003	vdx
MIME HTML	MHT
Rich Text Format 1 jusqu'à 1.7	RTF
Unicode Text 3, 4	TXT
XHTML 1.0	HTM, HTML
XML (générique)	XML

Tableau 13-11. Formats de traitement de texte

Format d'application	Extensions
Adobe FrameMaker InterchangeFormat 5, 5.5, 6, 7	MIF
Apple iChat Log AV, AV 2, AV 2.1, AV 3	LOG
Apple iWork Pages '08, 2009	GZ
Applix Words 3.11, 4, 4.1, 4.2, 4.3, 4.4	AW
Corel WordPerfect Linux 6.0, 8.1	WPS
Corel WordPerfect Macintosh 1.02, 2, 2.1, 2.2, 3, 3.1	WPS
Corel WordPerfect Windows 5, 5.1, 6, 7, 8, 9, 10, 11, 12, X3	WO, WPD
DisplayWrite 4	IP
Folio Flat File 3.1	FFF
Founder Chinese E-paper Basic 3.2.1	CEB
Fujitsu Oasys 7	OA2
Haansoft Hangul 97, 2002, 2005, 2007	HWP

Tableau 13-11. Formats de traitement de texte (suite)

Format d'application	Extensions
IBM DCA/RFT (Revisable Form Text) SC23-0758 -1	DC
JustSystems Ichitaro 8 jusqu'à 2009	JTD
Lotus AMI Pro 2, 3	SAM
Lotus AMI Professional Write Plus 2.1	AMI
Lotus Word Pro	96, 97, R9
Lotus SmartMaster 96, 97	MWP
Microsoft Word PC 4, 5, 5.5, 6	DOC
Microsoft Word Windows 1.0 et 2.0, 6, 7, 8, 95, 97, 2000, 2002, 2003	DOC
Microsoft Word Windows XML 2007	DOCX, DOTX, DOTM
Microsoft Word Macintosh 4, 5, 6, 98, 2001, v.X, 2004	DOC
Microsoft Works 2, 3, 4, 6, 2000	WPS
Microsoft Windows Write 1, 2, 3	WRI
Oasis Open Document Format 1, 2	ODT, SXW, STW
OpenOffice Writer 1, 1.1	SXW, ODT
Omni Outliner 3	OPML, OO3, OPML, OOUTLINE
Skype Log File	DBB
StarOffice Writer 6, 7	SXW, ODT
WordPad jusqu'à 2003	RTF
XML Paper Specification	XPS
XyWrite 4.12	XY4

Dépannage 14

Cette section vous guide dans la résolution des problèmes courants liés à vShield.

Ce chapitre aborde les rubriques suivantes :

- « Résoudre les problèmes d'installation de vShield Manager », page 123
- « Résoudre les problèmes de fonctionnement », page 124
- « Résoudre les problèmes liés à vShield Edge », page 126
- « Résoudre les problèmes liés à vShield Endpoint », page 127
- « Résolution des problèmes liés à vShield Data Security », page 128

Résoudre les problèmes d'installation de vShield Manager

Cette section fournit des informations détaillées sur la résolution des problèmes d'installation de vShield Manager.

Impossible d'installer le fichier OVA de vShield dans vSphere Client

Vous ne pouvez pas installer le fichier OVA vShield.

Problème

Quand j'essaie d'installer le fichier OVA de vShield, l'installation échoue.

Solution

Si un fichier OVA de vShield ne peut pas être installé, une fenêtre d'erreur dans vSphere Client indique la ligne où l'erreur s'est produite. Envoyez les informations de cette erreur avec la version de vSphere Client au support technique de VMware.

Connexion impossible à la CLI après le démarrage de la machine virtuelle vShield Manager

Problème

Je ne peux pas me connecter à la CLI de vShield Manager après avoir installé OVF.

Solution

Patientez quelques minutes après l'installation de vShield Manager pour vous connecter à la CLI de vShield Manager. Dans la vue de l'onglet Console, appuyez sur Entrée pour rechercher une invite de commande si l'écran est noir.

Connexion impossible à l'interface utilisateur de vShield Manager

Problème

Quand j'essaie de me connecter à l'interface utilisateur de vShield Manager depuis mon navigateur Web, une erreur Page introuvable s'affiche.

Solution

L'adresse IP de vShield Manager figure dans un sous-réseau auquel le navigateur Web ne peut pas accéder. L'adresse IP de l'interface de gestion du vShield Manager doit être accessible par le navigateur Web pour utiliser vShield.

Résoudre les problèmes de fonctionnement

Les problèmes de fonctionnement éventuels apparaissent après l'installation.

vShield Manager ne peut pas communiquer avec vShield App

Problème

Je n'arrive pas à configurer vShield App depuis vShield Manager.

Solution

Si c'est le cas, la connectivité est perdue entre les deux machines virtuelles. L'interface de gestion de vShield ne peut pas communiquer avec celle de vShield Manager. Vérifiez que les interfaces de gestion figurent sur le même sous-réseau. Vérifiez que les interfaces de gestion se trouvent dans le même VLAN (si ce type de réseau est utilisé).

La mise hors tension de la machine virtuelle vShield App ou vShield Manager peut également expliquer ce problème.

Impossible de configurer vShield App

Problème

Je n'arrive pas à configurer vShield App.

Solution

Ceci peut provenir de l'une des conditions suivantes.

- La machine virtuelle vShield App est endommagée. Désinstallez le module vShield App incriminé de l'interface utilisateur de vShield Manager. Installez-en un nouveau pour protéger l'hôte ESX.
- vShield Manager ne parvient pas à communiquer avec vShield App.
- Le système de stockage/LUN contenant le fichier de configuration de vShield est tombé en panne. Quand ceci arrive, vous ne pouvez pas effectuer des modifications de configuration. Le pare-feu continue cependant à fonctionner. Vous pouvez stocker les machines virtuelles vShield dans un stockage local si le stockage distant n'est pas fiable.

Prenez un snapshot ou créez un fichier TAR du vShield App concerné en utilisant vSphere Client. Envoyez ces informations au support technique de VMware.

La règle de blocage de pare-feu ne bloque pas le trafic correspondant

Problème

J'ai configuré une règle d'App Firewall pour bloquer le trafic spécifique. J'ai utilisé Flow Monitoring pour consulter le trafic, et celui que je voulais bloquer est autorisé.

Solution

Vérifiez l'ordre et l'étendue de la règle. Ceci comprend le niveau du conteneur pour l'application de la règle. Des problèmes peuvent survenir quand une règle sur adresse IP est configurée dans le mauvais conteneur.

Vérifiez l'emplacement de la machine virtuelle concernée. La machine virtuelle figure-t-elle derrière vShield App ? Si ce n'est pas le cas, aucun agent ne permet d'appliquer la règle. Sélectionnez la machine virtuelle dans l'arborescence de ressources. L'onglet App Firewall correspondant à cette machine virtuelle affiche toutes les règles qui concernent cette machine virtuelle.

Placez des machines virtuelles non protégées sur un commutateur protégé par vShield ou protégez le commutateur virtuel sur lequel se trouve la machine virtuelle en installant vShield.

Activez la journalisation de la règle d'App Firewall en question. Ceci peut ralentir le trafic réseau par l'intermédiaire de vShield App.

Vérifiez la connectivité de vShield App. Vérifiez si le module vShield App est désynchronisé sur la page System Status. Si c'est le cas, cliquez sur **[Force Sync]** . S'il n'est toujours pas synchronisé, allez dans le journal System Event pour en déterminer la cause.

Aucun flux de données ne s'affiche dans Flow Monitoring

Problème

J'ai installé vShield Manager et vShield App. Quand j'ai ouvert l'onglet Flow Monitoring, aucune donnée ne s'affichait.

Solution

Ceci peut provenir de l'une ou de plusieurs des conditions suivantes.

- Vous n'avez pas laissé suffisamment de temps à vShield App pour contrôler les sessions du trafic. Attendez quelques minutes après l'installation de vShield App pour collecter les données du trafic. Pour demander la collecte de données, cliquez sur **[Get Latest]** de l'onglet Flow Monitoring.
- Le trafic est destiné aux machines virtuelles non protégées par vShield App. Assurez-vous que les machines virtuelles sont protégées par vShield App. Les machines virtuelles doivent figurer dans le même groupe de ports que le port (p0) protégé par vShield App.
- Il n'existe aucun trafic vers les machines virtuelles protégées par vShield App.
- Recherchez les problèmes éventuels de désynchronisation dans l'état système de chaque vShield App.

Résoudre les problèmes liés à vShield Edge

Cette section fournit des informations détaillées sur la résolution des problèmes de fonctionnement liés à vShield Edge.

Les machines virtuelles n'obtiennent pas d'adresses IP auprès du serveur DHCP

Procédure

1. Vérifiez que la configuration de DHCP est réussie dans vShield Edge en exécutant la commande CLI : `show configuration dhcp`.
2. Vérifiez si le service DHCP est en cours d'exécution sur vShield Edge en exécutant la commande CLI : `show service dhcp`
3. Vérifiez que vmnic est actif sur la machine virtuelle et que vShield Edge est connecté (cases à cocher **[vCenter] > [Virtual Machine] > [Edit Settings] > [Network Adapter] > [Connected/Connect at Power On]**).

   Lors de l'installation de vShield App et de vShield Edge sur le même hôte ESX, les cartes réseau peuvent être déconnectées si vShield App est installé après vShield Edge.

L'équilibreur de charge ne fonctionne pas

Procédure

1. Vérifiez que l'équilibreur de charge est en cours d'exécution à l'aide de la commande CLI : `show service lb`.

   Vous pouvez démarrer l'équilibreur de charge en exécutant la commande `start`.
2. Vérifiez la configuration de l'équilibreur de charge à l'aide de la commande : `show configuration lb`.

   Cette commande indique également sur quelles interfaces externes les ports d'écoute sont exécutés.

L'équilibreur de charge génère l'erreur 502 passerelle incorrecte pour les demandes HTTP

Cette erreur se produit quand le serveur principal ou interne ne réagit pas aux demandes.

Procédure

1. Vérifiez que les adresses IP du serveur interne sont correctes.

   La configuration actuelle est visible à travers vShield Manager ou la commande CLI `show configuration lb`.
2. Vérifiez que les adresses IP du serveur interne sont accessibles à partir de l'interface interne de vShield Edge.
3. Vérifiez que les serveurs internes surveillent la combinaison IP:Port indiquée lors de la configuration de l'équilibreur de charge.

   Si aucun port n'est indiqué, IP:80 doit être sélectionné. Le serveur interne ne doit pas écouter uniquement 127.0.0.1:80 ; soit 0.0.0.0:80, soit <internal-ip>:80 doit être ouvert.

Le VPN ne fonctionne pas

Procédure

1 Vérifiez que l'autre extrémité du tunnel est configurée correctement.

Utilisez la commande de CLI : `show configuration ipsec`

2 Vérifiez que le service IPSec est en cours d'exécution sur vShield Edge.

Pour vérifier à l'aide de la commande CLI : `show service ipsec`. Le service IPSec doit être démarré à l'aide de la commande `start`.

Si ipsec est en cours d'exécution et que des erreurs se sont produites lors de la création du tunnel, la sortie de `show service ipsec` affiche des informations pertinentes.

3 Vérifiez la configuration aux deux extrémités (vShield Edge et remoteEnd), notamment les clés partagées.

4 Déboguez les problèmes liés à MTU ou à la fragmentation à l'aide de ping avec de petits et grands paquets.

- `ping –s 500 ip–at–end–of–the–tunnel`
- `ping –s 2000 ip–at–end–of–the–tunnel`

Résoudre les problèmes liés à vShield Endpoint

Cette section fournit des informations détaillées sur la résolution des problèmes de fonctionnement liés à vShield Endpoint.

Journalisation de l'agent léger

La journalisation de l'agent léger de vShield Endpoint est effectuée à l'intérieur des machines virtuelles. Deux valeurs de registre sont lues au démarrage depuis le registre Windows. Elles sont interrogées à nouveau périodiquement.

Les deux valeurs de registre `log_dest` et `log_level` se trouvent dans les emplacements suivants du registre :

- `HKLM\System\CurrentControlSet\Services\vsepflt\Parameters\log_dest`
- `HKLM\System\CurrentControlSet\Services\vsepflt\Parameters\log_level`

Toutes deux sont des masques de bits `DWORD` qui peuvent être une combinaison des valeurs suivantes :

Tableau 14-1. Journalisation de l'agent léger

DWORD	Valeur	Description
`log_dest`	`0x1`	`WINDBLOG`
	`0x2`	Nécessite un mode debug `VMWARE_LOG` Le fichier Log est stocké dans le répertoire racine de la machine virtuelle
`log_level`	`0x1`	`AUDIT`
	`0x2`	`ERROR`
	`0x4`	`WARN`
	`0x8`	`INFO`
	`0x10`	`DEBUG`

Par défaut, les valeurs des versions sont réglées sur VMWARE_LOG et sur AUDIT. Vous pouvez régler sur chacune des valeurs.

Pour plus d'informations sur la surveillance de l'intégrité de vShield Endpoint, voir Chapitre 12, « Événement et alarmes vShield Endpoint », page 69.

Compatibilité entre les versions de composants

Les versions de SVM et de l'agent léger doivent être compatibles.

Pour récupérer les numéros de versions des différents composants, procédez ainsi :

- SVM : Pour les SVM partenaires, veuillez vous référer aux instructions du fournisseur de la solution antivirus. Pour la machine virtuelle vShield Data Security, connectez-vous au vShield Manager et sélectionnez la machine virtuelle depuis l'inventaire. L'onglet Résumé indique le numéro de version.
- GVM : Cliquez à droite des propriétés des fichiers de pilotes pour obtenir le numéro de la version. Le chemin vers le pilote est le suivant : `C:\WINDOWS\system32\drivers\vsepflt.sys`.
- Module vShield Endpoint : Connectez-vous à vShield Manager et sélectionnez un hôte depuis l'inventaire. L'onglet Résumé indique le numéro de version de vShield Endpoint.

Vérifier l'intégrité et les alarmes vShield Endpoint

Les composants vShield Endpoint doivent pouvoir communiquer avec vShield Manager.

Procédure

1. Dans vSphere Client, accédez à **[Inventaire] > [Hôtes et clusters]** .
2. Sélectionnez un centre de données, un cluster ou un hôte ESX dans l'arborescence des ressources.
3. Cliquez sur l'onglet **[vShield App]** .
4. Cliquez sur **[Endpoint]** .
5. Vérifiez que la machine virtuelle de sécurité (SVM), le module vShield Endpoint résidant sur l'hôte ESX et l'agent léger résidant sur la machine virtuelle protégée sont normaux.
6. Si l'agent léger résidant sur la machine virtuelle n'est pas normal, vérifiez que la version de VMware Tools est 8.6.0 (commercialisée avec ESXi 5.0 Patch 1).
7. Si une alarme est affichée, exécutez l'action appropriée. Pour plus d'informations, voir « Alarmes vShield Endpoint », page 70.

Résolution des problèmes liés à vShield Data Security

Comme vShield Data Security utilise la technologie vShield Endpoint, le dépannage est pratiquement identique pour les deux composants.

Lorsque vous rencontrez un problème avec vShield Data Security, vérifiez d'abord que le dispositif de sécurité des données soit bien activé. Vérifiez ensuite que l'analyse de la sécurité des données avait été démarrée.

Vérifier l'horodateur du début et de la fin des analyses

vShield Data Security n'analyse que les machines virtuelles sous tension. La première étape de la résolution des problèmes vShield Data Security consiste à vérifier que la machine virtuelle a été analysée.

Procédure

1. Dans vSphere Client, allez dans **[Inventory] > [Hosts and Clusters]** .
2. Sélectionnez un centre de données, un hôte ESX ou une machine virtuelle dans l'arborescence des données.

3 Sélectionnez l'onglet **[Tasks and Events]** .

4 Recherchez Scan dans la colonne Name et vérifiez que l'analyse a été effectuée avec succès.

À propos de la précision de la détection des violations

La précision est mesurée par deux facteurs : rappel et précision. L'association idéale du rappel et de la précision vous permettra d'obtenir le contenu que vous avez besoin de sécuriser et rien d'autre. Toute détection du contenu est évaluée de deux façons : positive ou négative, et vrai ou faux (par exemple, ai-je identifié l'objet de ma recherche, mon identification était-elle correcte ?).

Il existe quatre résultats possibles qui ont les significations suivantes :

Tableau 14-2. Résultats de la détection du contenu

	Positif	Négatif
Vrai	Contenu sensible identifié correctement comme étant sensible.	Contenu non sensible identifié correctement comme étant non sensible.
Faux	Contenu non sensible identifié par erreur comme étant sensible.	Contenu sensible identifié par erreur comme étant non sensible.

Le rappel rassemble la fraction des documents qui sont pertinents pour la lame d'analyse du contenu.

- Un rappel élevé jette un vaste filet et rassemble tous les documents potentiellement sensibles. Un rappel trop élevé peut donner davantage de faux positifs. [Faux positif = document considéré comme étant sensible par la lame d'analyse de contenu et qui n'est en réalité pas sensible.]
- Un rappel bas est plus sélectif quant aux documents renvoyés comme étant sensibles. Un rappel trop bas peut donner davantage de faux négatifs. [Faux négatif = document considéré comme n'étant pas sensible par la lame d'analyse de contenu, mais qui EST en réalité sensible.]

La précision correspond au pourcentage de documents récupérés qui sont pertinents pour la recherche.

- Une haute précision peut réduire le nombre de faux positifs renvoyés.
- Une précision basse peut augmenter le nombre de faux positifs renvoyés.

La précision fait référence à la pertinence des résultats renvoyés. Par exemple, les documents qui ont déclenché la politique de la Norme en matière de sécurité des données de l'industrie des cartes de paiement (PCI DSS – Payment Card Industry Data Security Standard) contenaient-ils tous de réels numéros de carte de crédit, ou certains contenaient-ils des numéros UPC ou EAN qui étaient identifiés incorrectement comme étant des données PCI sensibles ? Une haute précision peut être obtenue par une recherche étroite et ciblée pour s'assurer que chaque élément récupéré du contenu est véritablement sensible.

Tableau 14-3. Précision et rappel

Facteur de précision	Mesure	Problème si la valeur est basse
Précision	Pourcentage de documents récupérés qui sont réellement pertinents.	Nombre accru de faux
Rappel	Pourcentage de tous les documents sensibles qui sont effectivement récupérés.	Nombre accru de faux négatifs

Index

A

alarmes d'hôte pour vShield Endpoint **70**
alarmes pour vShield Endpoint **70**
alarmes SVM pour vShield Endpoint **70**
App Firewall
  à propos des règles L4 et L2/L3 **60**
  ajout de règles depuis Flow Monitoring **56**
  ajout de règles L4 **64**
  Default Rules **60**
  hiérarchie des règles **61**
  planification de l'application de règles **61**
  revenir à la règle précédente **65**
  suppression de règles **65**

B

Backups
  planification **28**
  restauration **29**
  sur demande **27**

C

Certificat SSL **20**
Cluster Level Rules **61**
compte d'utilisateur admin **22**
connexion à vCenter Server **17**

D

Data Center High Precedence Rules **61**
Data Center Low Precedence Rules **61**
Data Security, stratégie, réglementations **74**
Data Security,rôles d'utilisateur **74**
date **19**
Default Rules **60, 61**
démarrage ou arrêt de services vShield Edge **47**
dépannage
  installation de vShield Manager **123**
  problèmes de fonctionnement **124**
  problèmes liés à vShield Edge **126**
  problèmes liés à vShield Endpoint **127**
DNS **18**
données
  programmation de sauvegardes **28**
  restauration d'une sauvegarde **29**
  sauvegardes sur demande **27**

E

équilibrage de charge **46**
espace de noms **59**
état
  de mise à jour **25**
  de vShield Manager **19**
  vShield App **50**
  vShield Edge **35**
  vShield Endpoint **69**
état de mise à jour **25**
état système
  Force Sync **50**
  Redémarrer **50**
  statistiques de trafic **51**
événements
  envoi à syslog **49**
  format Syslog **33**
  vShield App **32**
  vShield Manager **31**
événements pour vShield Endpoint **70**
événements système **31**

F

Flow Monitoring
  à propos **53**
  affichage d'une application spéciale **54**
  affichage du rapport **55**
  ajout d'une règle App Firewall **56**
  plage de dates **54**
  suppression de tous les flux enregistrés **56**
Force Sync **50**
format Syslog **33**
formats de fichier pris en charge **117**

G

groupes de sécurité
  à propos **60**
  ajouter **63**

H

heure **19**
heure système **19**
hiérarchie des règles App Firewall **61**

I

installation, mises à jour **25**
Interface utilisateur, connexion **13**
interface utilisateur, connexion **13**

J

journal de support technique **19**
journaux
  audit **33, 63**
  support technique **19**
journaux d'audit **33, 63**
journaux de support technique, vShield App **52**

L

Lame d'analyse de contenu des numéros de permis de conduire du Massachusetts **106**
lames d'analyse de contenu
  Lame d'analyse de contenu « ABN (numéro d'entreprise australien) » **98**
  Lame d'analyse de contenu « ACN (numéro de société australien) » **98**
  Lame d'analyse de contenu « American Express » **97**
  Lame d'analyse de contenu « Dates d'admission et d'autorisation de sortie » **96**
  Lame d'analyse de contenu « Données de piste de carte de crédit » **99**
  Lame d'analyse de contenu « Index des Procédures » **104**
  Lame d'analyse de contenu « ITIN non mis en forme » **105**
  Lame d'analyse de contenu « Numéro BIC allemand » **101**
  Lame d'analyse de contenu « Numéro BIC France » **101**
  Lame d'analyse de contenu « Numéro d'assurance sociale canadienne » **99**
  Lame d'analyse de contenu « Numéro d'identification national français » **101**
  Lame d'analyse de contenu « Numéro de carte de paiement de l'UE » **100**
  Lame d'analyse de contenu « Numéro de carte Medicare australienne » **98**
  Lame d'analyse de contenu « Numéro de compte bancaire australien » **97**
  Lame d'analyse de contenu « Numéro de compte personnalisé » **100**
  Lame d'analyse de contenu « Numéro de dossier fiscal australien » **98**
  Lame d'analyse de contenu « Numéro de passeport allemand » **102**
  Lame d'analyse de contenu « Numéro de permis de conduire canadien » **99**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'état d'Idaho » **103**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Californie » **98**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Floride » **100**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Géorgie » **101**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État de Hawaii » **102**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'état de l'Illinois » **103**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'état de l'Indiana » **103**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'état de l'Iowa » **104**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État du Colorado » **99**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État du Connecticut » **99**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'État du Delaware » **100**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'état du Kansas » **105**
  Lame d'analyse de contenu « Numéro de permis de conduire de l'état du Kentucky » **105**
  Lame d'analyse de contenu « Numéro de permis de conduire français » **100**
  Lame d'analyse de contenu « Numéro de permis de conduire italien » **104**
  Lame d'analyse de contenu « Numéro de TVA allemand » **102**
  Lame d'analyse de contenu « Numéro français de TVA » **101**
  Lame d'analyse de contenu « Numéro IBAN italien » **104**
  Lame d'analyse de contenu « Numéros d'assurance de groupe » **102**
  Lame d'analyse de contenu « Numéros d'identification nationaux allemands » **102**

Lame d'analyse de contenu « Numéros d'identification nationaux en Italie » **102**
Lame d'analyse de contenu « Permis de conduire de l'État d'Alabama » **96**
Lame d'analyse de contenu « Permis de conduire de l'État d'Alaska » **96, 97**
Lame d'analyse de contenu « Permis de conduire de l'État d'Arizona » **97**
Lame d'analyse de contenu « Permis de conduire de l'État de l'Arkansas » **96, 97**
Lame d'analyse de contenu « Permis de conduire de la Province d'Alberta » **96, 97**
Lame d'analyse de contenu de numéro de permis de conduire de Caroline du Sud **113**
Lame d'analyse de contenu de numéro de permis de conduire de l'Oklahoma **111**
Lame d'analyse de contenu de numéro de permis de conduire de l'Oregon **111**
Lame d'analyse de contenu de numéro de permis de conduire de l'Utah **116**
Lame d'analyse de contenu de numéro de permis de conduire de Pennsylvanie **111**
Lame d'analyse de contenu de numéro de permis de conduire de Rhode Island **112**
Lame d'analyse de contenu de numéro de permis de conduire de Virginie **116**
Lame d'analyse de contenu de numéro de permis de conduire de Washington **117**
Lame d'analyse de contenu de numéro de permis de conduire du Dakota du Sud **113**
Lame d'analyse de contenu de numéro de permis de conduire du Tennessee **115**
Lame d'analyse de contenu de numéro de permis de conduire du Wisconsin **117**
Lame d'analyse de contenu de numéro de permis de conduire du Wyoming **117**
Lame d'analyse de contenu de numéro de permis de conduire en Allemagne **101**
Lame d'analyse de contenu des conditions des informations protégées sur la santé **112**
Lame d'analyse de contenu des dictionnaires de formules du code national de drogue (NDC) **107**
Lame d'analyse de contenu des indices des praticiens de la santé en Nouvelle-Zélande **110**
Lame d'analyse de contenu des numéros d'assurance nationaux formels du Royaume-Uni **116**
Lame d'analyse de contenu des numéros d'assurance sociale formatés **112**
Lame d'analyse de contenu des numéros d'assurance sociale non formatés **113**
Lame d'analyse de contenu des numéros d'identification des patients **111**
Lame d'analyse de contenu des numéros d'identification nationale des Pays-Bas **108**
Lame d'analyse de contenu des numéros d'identification nationale espagnols **114**
Lame d'analyse de contenu des numéros de carte Visa **117**
Lame d'analyse de contenu des numéros de l'Indice National de la Santé en Nouvelle-Zélande **110**
Lame d'analyse de contenu des numéros de passeport des Pays-Bas **108**
Lame d'analyse de contenu des numéros de passeport du Royaume-Uni **116**
Lame d'analyse de contenu des numéros de passeport espagnol **114**
Lame d'analyse de contenu des numéros de passeport suédois **114**
Lame d'analyse de contenu des numéros de permis de conduire de Caroline du Nord **110**
Lame d'analyse de contenu des numéros de permis de conduire de l'état de New York **109**
Lame d'analyse de contenu des numéros de permis de conduire de l'Ohio **111**
Lame d'analyse de contenu des numéros de permis de conduire de Louisiane **105**
Lame d'analyse de contenu des numéros de permis de conduire des Pays-Bas **108**
Lame d'analyse de contenu des numéros de permis de conduire du Dakota du Nord **110**
Lame d'analyse de contenu des numéros de permis de conduire du Maine **105**
Lame d'analyse de contenu des numéros de permis de conduire du Maryland **106**
Lame d'analyse de contenu des numéros de permis de conduire du Michigan **106**

Lame d'analyse de contenu des numéros de permis de conduire du Minnesota **107**
Lame d'analyse de contenu des numéros de permis de conduire du Mississippi **107**
Lame d'analyse de contenu des numéros de permis de conduire du Missouri **107**
Lame d'analyse de contenu des numéros de permis de conduire du Montana **107**
Lame d'analyse de contenu des numéros de permis de conduire du Nebraska **107**
Lame d'analyse de contenu des numéros de permis de conduire du New Hampshire **109**
Lame d'analyse de contenu des numéros de permis de conduire du New Jersey **109**
Lame d'analyse de contenu des numéros de permis de conduire du Nouveau-Mexique **109**
Lame d'analyse de contenu des numéros de permis de conduire du Royaume-Uni **115**
Lame d'analyse de contenu des numéros de sécurité sociale espagnols **114**
Lame d'analyse de contenu des numéros de sécurité sociale formatés **113**
Lame d'analyse de contenu des numéros de sécurité sociale non formatés **113**
Lame d'analyse de contenu des numéros IBAN des Pays-Bas **108**
Lame d'analyse de contenu des numéros IBAN du Royaume-Uni **115**
Lame d'analyse de contenu des numéros IBAN suédois **114**
Lame d'analyse de contenu des permis de conduire de l'Île-du-Prince-Édouard **111**
Lame d'analyse de contenu des permis de conduire de l'Ontario **111**
Lame d'analyse de contenu des permis de conduire de la Nouvelle-Écosse **110**
Lame d'analyse de contenu des permis de conduire de Saskatchewan **112**
Lame d'analyse de contenu des permis de conduire de Terre-Neuve-et-Labrador **110**
Lame d'analyse de contenu des permis de conduire du Manitoba **106**
Lame d'analyse de contenu des permis de conduire du New Brunswick **109**
Lame d'analyse de contenu des permis de conduire du Québec **112**
Numéro de routage ABA **96**
Numéro de service des recettes fiscales de Nouvelle-Zélande **110**
login, vShield Manager **13**

M

messages d'audit pour vShield Endpoint **71**
mise à jour d'utilisateur **23**
mises à jour
état de mise à jour **25**
installation **25**
modification d'un compte utilisateur **23**
mot de passe **23**

N

NAT **40**
NTP **19**
numéro de série de vShield Manager **19**

P

panneau d'inventaire **14**
pare-feu
ajout de règles depuis Flow Monitoring **56**
ajout de règles L4 **64**
App Firewall, à propos **59**
planification de l'application de règles **61**
suppression de règles **65**
plage de dates d'analyse de trafic **54**
plage de dates de Flow Monitoring **54**
plage de dates pour Flow Monitoring **54**
plug-in **18**
plug-in vSphere **18**
programmation de sauvegardes **28**

R

rapports
événements système **31**
journal d'audit **33, 63**
redémarrage d'une vShield App **50**
rédéploiement d'un vShield Edge **47**
réglementations
Arizona SB-1338 **79**
California AB-1298 **81**
California SB-1386 **81**
Colorado HB-1119 **82**
Connecticut SB-650 **83**
FERPA (Loi sur les Droits de la famille et protection des données dans l'éducation) **84**
Florida HB-481 **84**
Illinois SB-1633 **87**
Massachusetts CMR-201 **89**
Minnesota HF-2121 **89**

Nevada SB-347 **90**
New Hampshire HB-1660 **90**
New Jersey A-4001 **91**
New York AB-4254 **91**
Norme de sécurité informatique des données de l'industrie des cartes de paiement (PCI-DSS) **93**
Numéros BIC du Royaume-Uni **93**
Numéros d'assurance nationaux du Royaume-Uni **94**
Numéros d'assurance sociale canadienne **82**
Numéros d'identification des patients **93**
Numéros de carte de crédit **83**
Numéros de carte de paiement de l'UE **84**
Numéros de carte Medicare australienne **80**
Numéros de compte bancaire australien **80**
Numéros de compte personnalisé **83**
Numéros de dossiers fiscaux australiens **81**
Numéros de passeport du Royaume-Uni **94**
Numéros de permis de conduire canadien **82**
Numéros de permis de conduire des Pays-Bas **90**
Numéros de permis de conduire du Royaume-Uni **94**
Numéros de routage ABA **79**
Numéros de sécurité sociale américains **95**
Numéros de service des recettes fiscales de Nouvelle-Zélande **91**
Numéros du ministère de la santé de Nouvelle-Zélande **92**
Numéros du Service national de santé (NHS) du Royaume-Uni **94**
Numéros IBAN du Royaume-Uni **94**
Ohio HB-104 **92**
Oklahoma HB-2357 **92**
Politique concernant la loi Hawaii SB-2290 **86**
Politique concernant la loi Idaho SB-1374 **87**
Politique concernant la loi Indiana HB-1101 **87**
Politique concernant la loi Kansas SB-196 **88**
Politique concernant les numéros BIC allemands **85**
Politique concernant les numéros d'identification nationaux allemands **86**
Politique concernant les numéros d'identification nationaux français **85**
Politique concernant les numéros d'identification nationaux italiens **88**
Politique concernant les numéros de permis de conduire en Allemagne **85**
Politique concernant les numéros de permis de conduire italien **88**
Politique concernant les numéros de TVA allemands **86**
Politique concernant les numéros IBAN allemands **85**
Politique concernant les numéros IBAN français **84**
Politique concernant les numéros IBAN italiens **88**
Politique Georgia SB-230 **85**
Politique HIPPA (Healthcare Insurance Portability and Accountability Act – Loi sur la responsabilité et la transférabilité de l'assurance maladie) **86**
Règle :Maine LD-1671 **89**
Règle des numéros de permis de conduire américain **94**
Règle Louisiana SB-205 **88**
Règle Montana HB-732 **90**
Texas SB-122 **93**
Utah SB-69 **95**
Vermont SB-284 **95**
Washington SB-6043 **95**
règles
  ajout de règles L4 à App Firewall **64**
  suppression de règles de App Firewall **65**
règles L2/L3, à propos **60**
règles L4
  à propos **60**
  ajout **64**
restauration de sauvegardes **29**
rôles et droits, à propos **21**

S

Secure Port Group Rules **61**
serveur Syslog **49**
services
  DNS **18**
  NTP **19**
SpoofGuard **65**
statistiques de trafic pour une vShield App **51**
suppression d'un utilisateur **24**
synchronisation avec vCenter **17**
synchronisation d'une vShield App **50**
syslog, vShield Edge **36**

U

utilisateurs
  changement d'un mot de passe **23**
  compte admin **22**
  modification **23**
  rôles et droits **21**
  suppression **24**

V

VPN
- ajouter un site homologue **44**
- configurer le service **43**
- configurer un certificat d'authentification **44**
- gérer **43**

vShield
- vShield App **9**
- vShield Edge **9**
- vShield Endpoint **9**
- vShield Manager **9**

vShield App
- à propos **9**
- envoi d'événements à un serveur syslog **49**
- état système **50**
- exlcure des machines virtuelles de la protection **51**
- forcing sync **50**
- mode Prévention de défaillance **51**
- notification en fonction des événements **32**
- redémarrer **50**
- statistiques de trafic **51**

vShield Data Security
- à propos **73**
- analyse **77**
- formats de fichier pris en charge **117**
- règle **74**
- rôles d'utilisateur **74**

vShield Edge
- à propos **9**
- ajout de règles NAT **40**
- démarrage ou arrêt de services **47**
- DHCP **41**
- équilibrage de charge **46**
- état **35**
  - règles de pare-feu
    - afficher par type **39**
    - ajouter **37**
    - changer la priorité **39**
    - gérer **36**
    - modifier **39**
    - supprimer **40**
- syslog **36**
- VPN **43**

vShield Endpoint
- à propos **9**
- alarmes **70**
- alarmes d'hôte **70**
- alarmes SVM **70**
- état **69**
- événements **70**
- messages d'audit **71**

vShield Manager
- à propos **9**
- Certificat SSL **20**
- connexion **13**
- date et heure **19**
- DNS **18**
- état **19**
- événements système **31**
- notification en fonction des événements **31**
- NTP **19**
- numéro de série **19**
- panneau d'inventaire **14**
- panneaux d'interface utilisateur **14**
- plug-in vSphere **18**
- programmation d'une sauvegarde **28**
- restauration d'une sauvegarde **29**
- sauvegardes sur demande **27**
- Support **19**
- synchronisation avec vCenter Server **17**

vue Hosts & Clusters **14**

vue Networks **14**

vue Secured Port Groups **14**

vues
- Hosts & Clusters **14**
- Networks **14**
- Secured Port Groups **14**